VMware NSX:
Install, Configure, Manage

Lab Manual
NSX 6.4

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

VMware NSX:
Install, Configure, Manage
Lab Manual
NSX 6.4
Part Number EDU-EN-NSXICM64-LAB (4/2018)

The training material is provided “as is,” and all express or implied conditions, representations, and warranties, including any implied warranty of merchantability, fitness for a particular purpose or noninfringement, are disclaimed, even if VMware, Inc., has been advised of the possibility of such claims. This training material is designed to support an instructor-led training course and is intended to be used for reference purposes in conjunction with the instructor-led training course. The training material is not a standalone training tool. Use of the training material for self-study without class attendance is not recommended.

These materials and the computer programs to which it relates are the property of, and embody trade secrets and confidential information proprietary to, VMware, Inc., and may not be reproduced, copied, disclosed, transferred, adapted or modified without the express written approval of VMware, Inc.

www.vmware.com/education

CONTENTS

Lab 1 Configuring NSX Manager

Objective: Verify the NSX Manager appliance settings and registration to a vCenter Server system

In this lab, you perform the following tasks:

1. Access Your Lab Environment
2. Review and Modify the NSX Manager Configuration
3. Verify That the vSphere Web Client Plug-In for NSX Manager Is Installed
4. Verify That the vSphere and NSX Licenses Are Valid
5. Clean Up for the Next Lab

Task 1: Access Your Lab Environment

You use Remote Desktop Connection to connect to your lab environment.

1. Using the information that is provided by your instructor, log in to your lab environment.

Task 2: Review and Modify the NSX Manager Configuration

You review and modify the VMware NSX® Manager™ deployment configurations.

In your lab environment, the NSX Manager appliance is predeployed and preconfigured. NSX Manager is also registered to VMware vCenter® Server Appliance™.

1. Log in to the NSX Manager user interface.

   a. In the task bar of the student desktop, click the **Firefox** shortcut.

   b. In the browser window, click the **NSX Managers** > **Site A-NSX Manager (SA-NSX-Manager-01)** bookmark.

   c. On the login page, log in as admin and enter the password VMware1!.

2. In the NSX Manager user interface, click **View Summary.**

3. View the current NSX Manager appliance's IP address, CPU, memory, and storage utilization.

   The IP address should be 172.20.10.42.

4. Verify that the vPostgres, RabbitMQ, and NSX Management Service services are running.

   The NSX Universal Synchronization Service and the SSH Service are stopped, which is expected.

5. Click **Start** to start the SSH Service.

6. Click **Yes** in the Start Service pop-up window.

7. Click the **Manage** tab in the top-left corner.

8. On the **Manage** tab, verify that **Settings** > **General** is selected in the left pane.

9. Click **Edit** to configure the Syslog server IP address as 172.20.10.10 and the port as 514.

10. From the drop-down menu select **UDP** as the protocol, and click **OK**.

11. Scroll down to Locale and verify that it is set to en-US.

12. In the left pane, select **Network**, and view the information in the General network settings pane and the DNS Servers settings pane.

13. Verify that network settings are configured correctly.

    - The host name should be sa-nsxmgr-01.

    - The IPv4 information address should be 172.20.10.42, the netmask should be 255.255.255.0, and the default gateway should be 172.20.10.10.

14. Scroll down to DNS Servers, and verify that the primary server is 172.20.10.10 and that Search Domains is set to vclass.local.

15. In the left pane under Components, select **NSX Management Service** and verify that the values are configured correctly.

    - Lookup Service URL: https://sa-vcpsc-01.vclass.local:443/lookupservice/sdk
    - SSO Administrator: administrator@vsphere.local
    - Status: Connected (with green dot icon)
    - vCenter Server: sa-vcsa-01.vclass.local
    - vCenter Server User Name: administrator@vsphere.local
    - vCenter Server Status: Connected (with a green dot icon)

16. If the Lookup Service status is not green, click **Edit**, reenter **`VMware1!`** for the password, and click **OK**.

17. When a pop-up window prompts you to trust the certificate, click **OK**.

    The status turns green after a moment.

Task 3: Verify That the vSphere Web Client Plug-In for NSX Manager Is Installed

You verify that VMware vSphere® Web Client is installed.

In your lab environment, the vSphere Web Client plug-in for NSX Manager is preinstalled and ready for use.

1. Open a new browser tab and click the **vSphere Site-A** > **vSphere Web Client (SA-VCSA-01)** bookmark.

2. When prompted, select the **Use Windows session authentication** check box and click **Login**.

3. Wait for the initial authentication to complete.

   The initial authentication might take several minutes to complete.

4. In vSphere Web Client, point to the **Home** icon and select **Networking & Security**.

5. In the Navigator pane, review the list of VMware NSX® features and select **Dashboard**.

6. In the middle pane, verify that your NSX Manager instances appear in the **NSX Manager** drop-down menu under Overview.

7. Click the down arrow next to **172.20.10.42 | Standalone**.

   You should see two NSX Manager instances in the list: 172.20.10.42 and 172.20.110.43.

   If your NSX Manager instances do not appear in the NSX Manager list, ask your instructor for help.

Task 4: Verify That the vSphere and NSX Licenses Are Valid

You determine whether the licenses for VMware vCenter Server®, VMware ESXi™ hosts, and NSX Manager are valid. If a certain license has expired, you add a valid temporary license.

Your instructor will provide the license keys.

1. In vSphere Web Client, point to the **Home** icon and select **Administration**.
2. In the Navigator pane, select **Licenses**.
3. In the middle pane, click the **Licenses** tab.
4. Scroll to the right to show the Expiration column, and verify the expiration status of vCenter Server, the ESXi host, and NSX licenses.
5. If your vCenter Server license is still valid, go to step 7.
6. If your vCenter Server license has expired, assign a new vCenter Server license key.
   a. Under the **Licenses** tab, click the green plus sign.

      The New Licenses window appears.

   b. In the **License key** text box, enter or paste the vCenter Server license key and click **Next**.
   c. In the **License name** text box, enter **`vCenter Server`** and click **Next**.
   d. On the Ready to complete page, click **Finish**.
   e. Click the **Assets** tab and click the **vCenter Server Systems** tab.
   f. Select all the vCenter Server systems.
   g. Click **All Actions** and select **Assign License**.
   h. In the Assign License panel, select the vCenter Server license key that you added and click **OK**.
7. If your host license is still valid, go to step 9.
8. If your host license has expired, assign a VMware vSphere® Enterprise Edition 6 license key to each ESXi host.
   a. On the **Licenses** tab, click the green plus sign.

      The New Licenses window appears.

   b. In the **License key** text box, enter or paste the vSphere license key and click **Next**.
   c. In the **License name** text box, enter **`vSphere`** and click **Next**.
   d. On the Ready to complete page, click **Finish**.
   e. In the middle pane, click the **Assets** tab and click the **Hosts** tab.

f. Select all the ESXi hosts.

g. Click **All Actions** and select **Assign License**.

h. Select the vSphere license key that you added and click **OK**.

9. If your VMware NSX® for vSphere® license is still valid, go to task 5.

10. If your NSX license has expired or is missing key, assign a VMware NSX® for vSphere® license.

    NSX for vShield Endpoint (CPUs) is not included.

    a. On the **Licenses** tab, click the green plus sign.

    The New Licenses window appears.

    b. In the **License key** text box, enter or paste the NSX license key and click **Next**.

    c. In the **License name** text box, enter **`NSX`** and click **Next**.

    d. On the Ready to complete page, click **Finish**.

    e. Click the **Assets** tab and click the **Solutions** tab.

    f. Select **NSX for vSphere**.

    g. Click **All Actions** and select **Assign License**.

    h. Select the NSX license key that you added and click **OK**.

    i. On the **Solutions** tab, verify that Yes appears in the Is Licensed column.

Task 5: Clean Up for the Next Lab

You prepare for the next lab.

1. Point to the **Home** icon at the top and select **Networking & Security**.
2. In the **VMware NSX Manager** tab of the browser, determine whether the session timed out.
3. If the session did not time out, click the gear icon on the far right of the screen and select **Logout**.

Lab 2 Configuring and Deploying an NSX Controller Cluster

Objective: Deploy an NSX Controller cluster

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Deploy an NSX Controller Instance
3. Verify That the First NSX Controller Instance Is Operational
4. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If your Internet Explorer window is closed, click the **Firefox** icon on the student desktop.
2. If you are not logged in to vSphere Web Client, click the **vSphere Web Client - (SA-VCSA-01)** bookmark in the browser window.
3. When prompted, select the **Use Windows session authentication** check box and click **Login**.
4. On the vSphere Web Client Home page, click **Networking & Security**.

Task 2: Deploy an NSX Controller Instance

You configure and deploy a VMware NSX® Controller™ instance.

NOTE

For lab purposes only, you deploy only one controller. In a production network, VMware requires that each NSX Controller cluster contain three controller nodes, regardless of the size of the NSX deployment.

1. In the Navigator pane, select **Installation and Upgrade**.
2. Click the **Management** tab.
3. In the NSX Controller nodes pane, click the green plus sign.
4. In the Add Controller dialog box, configure and deploy the first NSX Controller instance.
   a. In the **Add Controller** text box, enter **SA**.
   b. From the **NSX Manager** drop-down menu, select **172.20.10.42** (NSX Manager IPv4 address).
   c. From the **Datacenter** drop-down menu, select **SA-Datacenter**.
   d. From the **Cluster/Resource Pool** drop-down menu, select **SA-Management**.
   e. From the **Datastore** drop-down menu, select **SA-Shared-01-Remote**.
   f. From the **Host** drop-down menu, select **sa-esxi-01.vclass.local**.
   g. Leave the folder selection blank.
   h. Click the **Connected To > Select** link.
   i. In the Select Network dialog box, select **Distributed Portgroup** from the **Object Type** drop-down menu.
   j. In the Available Objects list, select **pg-SA-Management** and click **OK**.
   k. Click the **IP Pool** > **Select** link.
   l. At the bottom of the Select IP Pool dialog box, click the **New IP Pool** link.

m. In the **Add Static IP Pool** dialog box, click the green plus sign and add a new pool.

Option	Action
Name	Enter `Controller-Pool`.
Gateway	Enter **172.20.10.10**.
Prefix Length	Enter **24**.
Primary DNS	Leave blank.
Secondary DNS	Leave blank.
DNS Suffix	Leave blank.
Static IP Pool	Click the green plus sign, and enter the NSX Controller static IP pool range **172.20.10.240-172.20.10.250**.

n. Click **OK**.

o. In the Select IP Pool dialog box, select **Controller-Pool** and click **OK**.

p. In the Add Controller dialog box, enter **VMware1!VMware1!** in the **Password** and **Confirm password** text boxes.

q. Click **OK**.

5. Monitor the status of the NSX Controller deployment.

   a. In the NSX Controller nodes pane, view the Status column.

   b. Monitor the deployment until the status changes from Deploying to Connected.

   The deployment process might take a few minutes to complete.

Task 3: Verify That the First NSX Controller Instance Is Operational

You use vSphere Web Client and the NSX Controller command line to determine the operational status of the NSX Controller cluster after adding one node.

1. Point to the vSphere Web Client **Home** icon and select **Hosts and Clusters**.
2. In the Navigator pane, expand the inventory view of **SA-Datacenter** to show the clusters.
3. Click the **Refresh** icon next to the current logged-in user name.
4. Expand the inventory view of the SA-Management-01 cluster, and select the newly deployed NSX Controller virtual machine.

   The virtual machine name starts with SA-NSX-controller-1.
5. In the middle pane, review the **Summary** tab report.

   Q1. What is the power status of the NSX Controller instance?

   Q2. How many vCPUs does the NSX Controller instance have?

   Q3. How much total memory does the NSX Controller instance have?

   Q4. How large is the NSX Controller hard disk?

   Q5. What port group is the NSX Controller instance connected to?

   Q6. What is the IP address of the NSX Controller instance?
6. Record the NSX Controller IP address. __________
7. Minimize the browser window.

8. Use MTPuTTY to establish an SSH connection to the first NSX Controller instance.

   a. In the student desktop task bar, click the **MTPuTTY** shortcut.

   b. Select **Server** on the top-left corner and click **Add Server**

   c. In the Properties window, enter the IP address that you recorded in step 6 in the **Server name** text box and select **SSH** as the protocol.

   d. In the **Display name** text box, enter **`Controller-1`**.

   e. Click **OK**.

      Your newly added controller appears on the left side.

   f. Double-click **Controller-1** in the list.

   g. If prompted to confirm a PuTTY security alert, click **Yes**.

   h. Log in as admin and enter the password **`VMware1!VMware1!`**.

9. In the MTPuTTY window, determine the cluster status for the first node.

   ```
   show control-cluster status
   ```

10. Review the command output.

    You might need to scroll up in the console window to find the answers.

    Q7. How many enabled and activated roles are listed?

    Q8. Can NSX Controller be safely restarted?

11. Determine the startup nodes in the cluster, and review the command output.

    ```
    show control-cluster startup-nodes
    ```

12. Review a detailed cluster role report.

    ```
    show control-cluster roles
    ```

13. Review the command output.

    Q9. How many roles were assigned with the first NSX Controller instance as master?

14. Review a cluster connections report.

    ```
    show control-cluster connections
    ```

15. Review the command output.

Q10. How many roles have components actively listening on a network port?

Q11. How many unique ports are used for role-based communications?

16. Close the MTPuTTY window.
17. Restore the browser window.

Task 4: Clean Up for the Next Lab

You prepare for the next lab.

1. Return to the browser, and point to the **Home** icon and select **Networking & Security**.

Lab 3 Preparing for Virtual Networking

Objective: Install the NSX for vSphere modules in ESXi hosts, and configure the VXLAN IP pools and a transport zone

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Install NSX for vSphere Modules on the ESXi Hosts
3. Configure VXLAN on the ESXi Hosts
4. Configure the VXLAN ID Pool
5. Configure a Local Transport Zone
6. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If the Firefox window is closed, click the **Firefox** icon in the student desktop task bar.
2. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
3. When prompted, select the **Use Windows session authentication** check box and click **Login**.
4. On the vSphere Web Client Home page, point to the **Home** icon and select **Networking & Security**.

Task 2: Install NSX for vSphere Modules on the ESXi Hosts

You install the NSX for vSphere modules on the ESXi hosts that are assigned to two different clusters.

1. In the Navigator pane, select **Installation and Upgrade**.
2. In the middle pane, click the **Host Preparation** tab.
3. Verify that **172.20.10.42** is selected from the **NSX Manager** drop-down menu.

   The SA-Management and the SA-Compute-01 clusters are listed.
4. For each listed cluster (SA-Management cluster and SA-Compute cluster-01), point to **Not Installed** in the Installation Status column, click the gear icon, and select **Install**.
5. When prompted with the `Are you sure you want to continue with the install` message, click **Yes**.
6. Monitor the installation status of each cluster.

   When installation is complete, Installation Status changes from Installing to a green check mark with the version number.

   The VXLAN column contains an active **Not Configured** link.
7. If Installation Status displays Not Ready, point to **Not Ready** in the Installation Status column, click the gear icon, and select **Resolve**.

   You might have to repeat this action before the Installation Status changes from Installing to a green check mark with the version number. If you have to repeat this action more than twice, tell your instructor.

Task 3: Configure VXLAN on the ESXi Hosts

For each cluster, you specify the distributed switch and the IP pool to be used for VXLAN networking.

1. For the SA-Compute-01 cluster, click the **Not Configured** link in the VXLAN column to open the Configure VXLAN networking dialog box.
2. Verify that the Switch selection is **dvs-SA-Datacenter**.
3. Verify that the VLAN setting is 0.
4. Verify that the MTU setting is 1600.
5. For VMKNic IP Addressing, click **Use IP Pool**.
6. Select **New IP Pool** from the **IP Pool** drop-down menu.

7. In the Add Static IP Pool dialog box, configure an IP pool.

Option	Action
Name	Enter **`VTEP-Pool`**.
Gateway	Enter the VTEP gateway IP address **`172.20.11.10`**.
Prefix Length	Enter **`24`**.
Primary DNS	Leave blank.
Secondary DNS	Leave blank.
DNS Suffix	Leave blank.
Static IP Pool	Click the green icon and enter **`172.20.11.150-172.20.11.160`**. This range is the IP address range for VTEPs.

8. Click **OK**.
9. Leave VMKNic Teaming Policy as **Fail Over**.
10. Leave the VTEP value as **1** and click **OK**.
11. Wait for the update to complete, and click the **Refresh** icon.
12. Verify that the SA-Compute-01 cluster VXLAN status is Configured, with a green check mark.
13. For the SA-Management cluster, click the **Not Configure**d link in the VXLAN column to open the Configure VXLAN networking dialog box.
14. Verify that the Switch selection is **dvs-SA-Datacenter**.
15. Verify that the VLAN setting is 0.
16. Verify that the MTU setting is 1600.
17. For VMKNic IP Addressing, click **Use IP Pool** and select **VTEP-Pool** from the drop-down menu.
18. Leave VMKNic Teaming Policy as **Fail Over**.
19. Leave the VTEP value as **1**.
20. Click **OK**.
21. Wait for the update to complete, and click the vSphere Web Client **Refresh** icon.
22. Verify that the SA-Management cluster VXLAN status is now Configured with a green check mark.

23. If the VXLAN status still shows Not Configured, wait and refresh again until the status changes.
24. Click the **Logical Network Preparation** tab and ensure that **VXLAN Transport** is selected.
25. In the **Clusters & Hosts** column, expand the view of each cluster.
26. Confirm that each host has a vmk2 interface, and record each host's vmk2 IP address.
    - sa-esxi-01.vclass.local __________ (vmk2 IP address)
    - sa-esxi-02.vclass.local __________ (vmk2 IP address)
    - sa-esxi-04.vclass.local __________ (vmk2 IP address)
    - sa-esxi-05.vclass.local __________ (vmk2 IP address)
27. Review the configuration information shown.

Q1. What is the number of VTEPs on each host? (Adjust the column width as necessary to show all columns.)

Q2. Which is the switch that is connected to each host's VMKNic?

Task 4: Configure the VXLAN ID Pool

You configure the ID range that is used to identify VXLAN networks.

1. On the **Logical Network Preparation** tab, click **Segment ID**.
2. Click **Edit** to open the Segment ID pool dialog box and configure settings.

Option	Action
Segment ID Pool	Enter **`5000-5999`**.
Enable multicast addressing	Leave the check box deselected.

3. Click **OK**.

Task 5: Configure a Local Transport Zone

You create and configure a local transport zone that controls which hosts the logical switch can reach.

1. On the **Logical Network Preparation** tab, click **Transport Zones**.
2. Click the green plus sign to open the New Transport Zone dialog box and configure a transport zone.

Option	Action
Name	Enter **`Local-Transport-Zone`**.
Replication Mode	Ensure that **Unicast** is clicked.
Select clusters that will be part of the Transport Zone	Select the check box for each cluster.

3. Click **OK**.
4. After the transport is created, verify that Local-Transport-Zone appears in the transport zones list with a control plane mode of unicast.
5. Verify that the VMkernel adapters were created for each host VTEP by pointing to the vSphere Web Client **Home** icon and selecting **Hosts and Clusters**.
6. In the Navigator pane, expand the inventory view of **SA-Datacenter** to display the clusters and hosts.

   NOTE

   The hosts display an alert regarding lost network uplink redundancy as a result of using one interface for the VXLAN VTEP. Click **reset to green** and **acknowledge**.

7. Select each host one at a time, and click the **Configure** tab.
8. Click **VMkernel adapters** in the middle pane.
9. In the VMkernel adapters display pane, find vmk2 in the device column.

   In the Network label, the value displayed should start with vxw-vmknicPg-dvs-.

   In the IP Address column, the VMkernel adapter should contain one of the addresses recorded in task 3, step 26.

Task 6: Clean Up for the Next Lab

You prepare for the next lab.

1. In vSphere Web Client, return to the Networking & Security view.

Lab 4 Configuring Logical Switch Networks

Objective: Create and test logical switches for the Web-Tier, App-Tier, and DB-Tier transport networks

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Create Logical Switches
3. Verify That Logical Switch Port Groups Appear in vSphere
4. Migrate Virtual Machines to Logical Switches
5. Test Network Connectivity
6. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
2. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
3. When prompted, select the **Use Windows session authentication** check box and click **Login**.
4. On the vSphere Web Client Home page, click **Networking & Security**.

Task 2: Create Logical Switches

You create logical switches for the Transit, Web-Tier, App-Tier, and DB-Tier networks.

1. In the Navigator pane, select **Logical Switches**.
2. In the middle pane, ensure that the **NSX Manager** drop-down menu is set to **172.20.10.42**.
3. In the middle pane, click the green plus sign to open the New Logical Switch dialog box.
4. Configure the Transit-Network switch.

    a. In the **Name** text box, enter **`Transit-Network`**.

    b. For Transport Zone, click **Change**.

    c. Verify that **Local-Transport-Zone** is selected and click **OK**.

       The replication mode automatically changes to unicast.

    d. Leave **Enable IP Discovery** selected and click **OK**.

5. Wait for the update to complete, and verify that Transit-Network appears with a status of Normal.
6. Click the green plus sign to open the New Logical Switch dialog box
7. Configure the Web-Tier switch.

    a. Enter **`Web-Tier`** in the **Name** text box.

    b. For Transport Zone, click **Change**.

    c. Verify that **Local-Transport-Zone** is selected and click **OK**.

    d. Leave **Enable IP Discovery** selected and click **OK**.

8. Wait for the update to complete and verify that Web-Tier appears with a status of Normal.
9. Click the green plus sign to create a logical switch.
10. In the New Logical Switch dialog box, configure the App-Tier switch.

    a. Enter **`App-Tier`** in the **Name** text box.

    b. For Transport Zone, click **Change**.

    c. Verify that **Local-Transport-Zone** is selected and click **OK**.

    d. Leave **Enable IP Discovery** selected and click **OK**.

11. Wait for the update to complete and verify that App-Tier appears with a status of Normal.
12. Click the green plus sign to create a logical switch.

13. In the New Logical Switch dialog box, configure the DB-Tier switch.

    a. Enter **`DB-Tier`** in the **Name** text box.

    b. For Transport Zone, click **Change**.

    c. Verify that **Local-Transport-Zone** is selected and click **OK**.

    d. Leave `Enable IP Discovery` selected and click **OK**.

14. Wait for the update to complete and verify that DB-Tier appears with a status of Normal.

Task 3: Verify That Logical Switch Port Groups Appear in vSphere

You verify that logical switch port groups appear in the vSphere networking inventory.

1. Point to the vSphere Web Client **Home** icon and select **Networking**.

2. Expand the Networking inventory tree.

3. Click the vSphere Web Client **Refresh** icon.

4. Drag the pane divider to the right to expand the horizontal size of the inventory pane so that the port group names appear completely.

5. In the dvs-SA-Datacenter inventory, find the port groups with names that end with certain suffixes.

   The names end with the following suffixes:

   - Transit-Network
   - Web-Tier
   - App-Tier
   - DB-Tier

6. If the specified port groups do not appear in the dvs-SA-Datacenter inventory, wait a minute and refresh vSphere Web Client.

7. Review the networking inventory.

   Q1. Can the ID number associated with a VXLAN logical switch be determined from the port group name?

Task 4: Migrate Virtual Machines to Logical Switches

You use the vSphere Web Client plug-in for NSX Manager to migrate virtual machines to logical switches.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the Navigator pane, select **Logical Switches**.
3. In the middle pane, select the **Web-Tier** logical switch.
4. Click **Actions** and select **Add VM.**
5. In the Web-Tier - Add Virtual Machines dialog box, migrate web virtual machines to the Web-Tier logical switch.
    a. In the Available Objects list, select **web-sv-01a** and **web-sv-02a**.
    b. Click the right arrow.
    c. Click **Next**.
    d. In the Select vNICs list, select the **web-sv-01a - Network Adapter 1 (VM-Network)** and **web-sv-02a - Network Adapter 1 (VM-Network)** check boxes.
    e. Click **Next**.
    f. Click **Finish**.
6. In the Logical Switches list, double-click the **Web-Tier** entry to manage that object.
7. Click the **Related Objects** tab and click **Virtual Machines**.

    Q1. Do the web-sv-01a and web-sv-02a virtual machines appear in the virtual machines list?

    Q2. Do any other virtual machines appear in the list?

8. At the top of vSphere Web Client, point to the **Home** icon and select **Networking & Security**.
9. In the Logical Switches list, select the **App-Tier** logical switch.
10. Click **Actions** and select **Add VM**.
11. In the Add Virtual Machines dialog box, migrate the app virtual machine to the App-Tier logical switch.
    a. In the Available Objects list, select **app-sv-01a**.
    b. Click the right arrow.

c. Click **Next**.

d. In the Select vNICs list, select the **app-sv-01a - Network Adapter 1 (VM Network)** check box.

e. Click **Next**.

f. Click **Finish**.

12. In the Logical Switches list, select the **DB-Tier** logical switch.

13. Click **Actions** and select **Add VM**.

14. In the Add Virtual Machines dialog box, migrate the database virtual machine (db-sv01a) to the DB-Tier logical switch.

    a. In the Available Objects list, select the **db-sv-01a**.

    b. Click the right arrow.

    c. Click **Next**.

    d. In the Select VNICs list, select the **db-sv-01a - Network Adapter 1 (VM Network)** check box.

    e. Click **Next**.

    f. Click **Finish**.

Task 5: Test Network Connectivity

You use virtual switch monitoring tools to test connectivity between virtual machines, between a physical system and the virtual machines, and between hosts.

1. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.

2. Expand the VMs and Templates inventory tree for sa-vcsa-01.vclass.local.

   Under Site-A-Datacenter, several virtual machines are found in the `Discovered virtual machine` folder, including:

   - web-sv-01a
   - web-sv-02a
   - app-sv-01a
   - db-sv-01a

3. Power on each of the virtual machines listed in step 2.

   a. Select the virtual machine in the inventory.

   b. From the **Actions** drop-down menu, select **Power** > **Power On**.

4. When each virtual machine is completely powered on, record their assigned IP addresses.

   - web-sv-01a __________
   - web-sv-02a __________
   - app-sv-01a __________
   - db-sv-01a __________

   To view an IP address assignment, you can select the virtual machine in the inventory. The IP address assignment appears at the top of the **Summary** tab report.

   The IP address information is also provided in your lab topology handout on the Lab Networks and IP Addressing page.

5. Use a console window to test connectivity from the web-sv-01a virtual machine.

   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.

   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.

   c. Click the **Summary** tab.

   d. Click the console thumbnail image.

   e. Log in with the user name root and the password VMware1!.

   f. At the command prompt, run the `arp -an` command to query the ARP cache.

   Q1. Did the command return any entries?

   g. At the command prompt, ping the IP address of web-sv-02a, which you recorded in step 4.

   ```
   ping IP_address
   ```

   Q2. Did the ping command receive replies from the web-sv-02a virtual machine?

   h. Press Ctrl+C to stop running the `ping` command.

   i. At the command prompt, query the ARP cache.

   ```
   arp -an
   ```

   Q3. Did the command return any entries?

j. At the command prompt, ping the IP address of app-sv-01a, which you recorded in step 4.

```
ping IP_address
```

Q4. Did the ping command receive replies from the app-sv-01a virtual machine?

k. Press Ctrl+C to stop the `ping` command.

l. At the command prompt, ping the IP address of db-sv-01a, which you recorded in step 4.

```
ping IP_address
```

Q5. Did the ping command receive replies from the db-sv-01a virtual machine?

m. Press Ctrl+C to stop the `ping` command.

n. Review the `ping` tests.

Q6. If any ping test failed, what might be the root cause?

o. In the browser window, press Ctrl+Alt to release the pointer.

p. Leave the web-sv-01a console window open for the remainder of the class.

6. Test connectivity between the VTEPs of ESXi hosts.

a. Minimize the browser and open MTPuTTY.

b. Double-click **SA-ESXi-01**.

c. In the PuTTY Security Alert pop-up window, click **Yes**.

A session is opened to connect to the ESXi host.

d. Ping from host sa-esxi-01 to host sa-esxi-04.

```
vmkping ++netstack=vxlan -d -s 1572 -I vmk2 sa-esxi-04_vmk2_address
```

Use the information that you recorded in lab 3, task 3, steps 24 through 26 to complete *sa-esxi-04_vmk2_address* in the command.

The `ping` command should be successful. This success indicates that the VTEPs on the hosts sa-esxi-01 and sa-esxi-04 can communicate with each other and that the physical network is configured to support VXLAN frames.

e. Using the information recorded in substep d, perform this test between sa-esxi-01 and hosts sa-esxi-02 and sa-esxi-03 to validate the VTEP connectivity of all the hosts.

Task 6: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Restore the browser window and return to the vSphere Web Client Networking & Security view.
2. In the browser, leave the web-sv-01a console window tab open.
3. On the student desktop, leave the MTPuTTY windows open.

Lab 5 Configuring and Deploying an NSX Distributed Router

Objective: Configure east-west routing by deploying a distributed logical router

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Configure and Deploy an NSX Distributed Logical Router
3. Verify the Distributed Router Deployment and Configuration
4. Test Connectivity
5. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. In the task bar of the student desktop, click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the Firefox window is closed, double-click the **Firefox** icon in the task bar of the student desktop.
3. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
4. When prompted, click the **Use Windows session authentication** check box and click **Login**.

5. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.

Task 2: Configure and Deploy an NSX Distributed Logical Router

You configure and deploy an NSX distributed logical router that is connected to each of the logical switches.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the Navigator pane, select **NSX Edges**.
3. In the middle pane, ensure that the **NSX Manager** drop-down menu is set to **172.20.10.42**.
4. In the middle pane, click the green plus sign to open the New NSX Edge dialog box.
5. On the Name and description page, click **Logical Router** for Install Type.
6. In the **Name** text box, enter **`Distributed-Router`** and click **Next**.
7. On the Settings page, leave User Name as admin, and enter **`VMware1!VMware1!`** in the **password** text box and the **Confirm password** text box.
8. Select the **Enable SSH Access** check box and click **Next**.
9. On the Configure Deployment page, verify that SA-Datacenter is selected.
10. Under NSX Edge Appliances, click the green plus sign to open the Add NSX Edge Appliance dialog box.
11. From the **Cluster/Resource Pool** drop-down menu, select **SA-Management**.
12. From the **Datastore** drop-down menu, select **SA-Shared-01-Remote**.
13. From the **Host** drop-down menu, select **sa-esxi-02.vclass.local**.
14. Leave all other fields blank and click **OK**.
15. Click **Next**.
16. On the Configure interfaces page, click the **Connected To > Select** link under HA Interface Configuration.

17. In the Connect NSX Edge to a Network dialog box, click **Distributed Virtual Portgroup**.

18. Click **pg-SA-Management** and click **OK**.

19. On the Configure interfaces page, click the green plus sign to open the Add Interface dialog box and configure the first of the four interfaces.

    a. Enter **`Transit-Network`** in the **Name** text box.

    b. For Type, leave **UpLink** selected.

    c. Click the **Connected To** > **Select** link.

    d. Click **Transit-Network** and click **OK**.

    e. Under Configure Subnets, click the green plus sign.

    f. Enter **`10.1.100.2`** in the **Primary IP Address** text box.

       10.1.100.2 is the IP address for the Transit-Network logical interface.

    g. Enter **`27`** in the **Subnet prefix length** text box.

    h. Leave all other settings at their default value and click **OK**.

20. On the Configure interfaces page, click the green plus sign to open the Add Interface dialog box and configure the second of the four interfaces.

    a. Enter **`Web-Tier`** in the **Name** text box.

    b. For Type, click **Internal**.

    c. Click the **Connected To** > **Select** link.

    d. Under the Logical Switch tab, click **Web-Tier** and click **OK**.

    e. Under Configure subnets, click the green plus sign.

    f. Enter **`10.1.10.1`** in the **IP Address** text box.

       10.1.10.1 is the IP address for the Web-Tier logical interface.

    g. Enter **`24`** in the **Subnet prefix length** text box.

    h. Leave all other settings at their default value and click **OK**.

21. On the Configure interfaces page, click the green plus sign to open the Add Interface dialog box and configure the third of the four interfaces.

    a. Enter **`App-Tier`** in the **Name** text box.

    b. For Type, click **Internal**.

    c. Click the **Connected To** > **Select** link.

    d. Click **App-Tier** and click **OK**.

    e. Click the green plus sign under Configure Subnets.

f. Enter **`10.1.20.1`** in the **IP Address** text box.

   10.1.20.1 is the IP address for the App-Tier logical interface.

g. Enter **`24`** in the **Subnet prefix length** text box.

h. Leave all other settings at their default value and click **OK**.

22. Under Configure Interfaces of this NSX Edge, click the green plus sign to open the Add Interface dialog box and configure the fourth interface.

    a. Enter **`DB-Tier`** in the **Name** text box.

    b. For Type, click **Internal**.

    c. Click the **Connected To** > **Select** link.

    d. Click **DB-Tier** and click **OK**.

    e. Click the green plus sign under Configure Subnets.

    f. Enter **`10.1.30.1`** in the **IP Address** text box.

       10.1.30.1 is the IP address for the DB-Tier logical interface.

    g. Enter **`24`** in the **Subnet prefix length** text box.

    h. Leave all other settings at the default value and click **OK**.

23. Compare the interface configurations to those in the table.

Name	IP Address	Subnet Prefix Length	Connected To
Transit-Network	10.1.100.2	27	Transit-Network
Web-Tier	10.1.10.1	24	Web-Tier
App-Tier	10.1.20.1	24	App-Tier
DB-Tier	10.1.30.1	24	DB-Tier

24. If an entry is not configured correctly, select the entry and click the pencil icon to edit the entry.

25. Click **Next**.

26. On the Default gateway settings page, deselect **Configure Default Gateway** and click **Next**.

27. On the Ready to complete page, review the configuration report and click **Finish**.

28. Above the edge list, monitor the deployment to completion.

    The deployment is complete when 0 installations are active.

Task 3: Verify the Distributed Router Deployment and Configuration

You verify that the distributed router is configured correctly and is deployed successfully.

1. In the NSX Edges list, verify that the Distributed Router entry is listed and the type is shown as Logical Router.
2. Double-click the **Distributed Router** entry to manage that object.
3. Click the **Manage** tab and click the **Settings** tab.
4. In the Settings category panel, select **Interfaces** to display the interface list of this NSX Edge instance.
5. In the Status column, verify that each interface has a green check mark.
6. In the Settings category panel, select **Configuration**.
7. At the bottom of the middle pane, find the Logical Router Appliances panel.

   Q1. On which datastore is the logical router Edge Appliance deployed?

   Q2. On which host is the logical router Edge Appliance running?

8. Point to the vSphere Web Client **Home** icon and select **Hosts and Clusters**.
9. Expand the inventory tree of SA-Datacenter so that all the inventory for each cluster appears.
10. In the inventory tree, find and select the Distributed Router appliance in the Management and Edge cluster.

    The appliance virtual machine name starts with Distributed Router and is followed by a number, for example, Distributed Router-0.

11. In the middle pane, click **Summary** to review the report.

12. Expand the **VM Hardware** section in the middle pane to view the hardware settings.

    Q3. How many vCPUs does the virtual machine have?

    Q4. How much memory does the virtual machine have?

    Q5. How large is hard disk 1?

    Q6. How large is hard disk 2?

    Q7. How many network adapters are connected to port groups?

Task 4: Test Connectivity

You use virtual switch monitoring tools to test connectivity between virtual machines, between a physical system and the virtual machines, and between hosts.

1. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.

2. Test connectivity from the web-sv-01a virtual machine.

   a. Open the console to the web-sv-01a virtual machine.

   b. At the command prompt, ping the web-sv-02a virtual machine.

   ```
   ping IP_address
   ```

   IP_address is 10.1.10.12.

   Q1. Did the ping command receive replies from the web-sv-02a virtual machine?

   c. Press Ctrl+C to stop the `ping` command.

   d. At the command prompt, ping the app-sv-01a virtual machine.

   ```
   ping IP_address
   ```

   IP_address is 10.1.10.1.

   Q2. Did the ping command receive replies from the app-sv-01a virtual machine?

e. Press Ctrl+C to stop the `ping` command.

f. At the command prompt, ping the db-sv-01a virtual machine.

```
ping IP_address
```

IP_address is 10.1.30.11.

Q3. Did the ping command receive replies from the db-sv-01a virtual machine?

g. Press Ctrl+C to stop the `ping` command.

h. Review the results of the `ping` tests.

Q4. Do these results differ from the ping tests you performed after creating the logical switches before adding the distributed router?

i. At the command prompt, query the ARP cache.

```
arp -an
```

Q5. Did the command return any entries?

j. Press Ctrl+Alt to release the pointer.

k. Click the **vSphere Web Client** tab.

3. Use a Command Prompt window to test connectivity from the student desktop system.

a. Minimize the browser window.

b. From the student desktop Command Prompt window, ping the web-sv-01a virtual machine.

```
ping IP_address
```

IP_address is 10.1.10.11.

Q6. Did the ping command receive replies from the web-sv-01a virtual machine?

c. From the student desktop Command Prompt window, ping the web-sv-02a virtual machine.

```
ping IP_address
```

IP_address is 10.1.10.12.

Q7. Did the ping command receive replies from the web-sv-02a virtual machine?

Q8. If no ICMP replies were received during the preceding tests, why not?

d. Leave the Command Prompt window open.

Task 5: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Restore the browser window.
2. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
3. In the browser window, leave the **vSphere Web Client** tab open.
4. Leave the web-sv-01a console window open.
5. On the student desktop, leave the Command Prompt and MTPuTTY windows open.

Lab 6 Deploying an NSX Edge Services Gateway and Configuring Static Routing

Objective: Configure and deploy an NSX Edge services gateway to provide perimeter routing

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Configure and Deploy an NSX Edge Services Gateway
3. Verify the NSX Edge Services Gateway Deployment
4. Configure Static Routes on the NSX Edge Services Gateway
5. Configure Static Routes on the Distributed Router
6. Test Connectivity Between an External Network and a Logical Switch Network
7. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. On the student desktop, click the **Command Prompt** shortcut in the task bar.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.

3. If you are not logged in to vSphere Web Client, click the **vSphere-Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
4. When prompted, select the **Use Windows session authentication** check box and click **Login**.
5. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in browser.

Task 2: Configure and Deploy an NSX Edge Services Gateway

You configure and deploy an NSX Edge services gateway to provide north-south routing and other network services.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the Navigator pane, select **NSX Edges**.
3. In the middle pane, click the green plus sign to open the New NSX Edge dialog box.
4. On the Name and description page, leave **Edge Services Gateway** selected for Install Type.
5. In the **Name** text box, enter `Perimeter-Gateway` and click **Next**.
6. On the Settings page, leave **User Name** as admin, and enter **`VMware1!VMware1!`** in the **password** text box and the **Confirm password** text box.
7. Select the **Enable SSH access** check box and click **Next**.
8. On the Configure deployment page, verify that **SA-Datacenter** is selected.
9. Verify that the Appliance Size selection is **Compact**.
10. Under NSX Edge Appliances, click the green plus sign to open the Add NSX Edge Appliance dialog box.
11. From the **Cluster/Resource Pool** drop-down menu, select **SA-Management**.
12. From the **Datastore** drop-down menu, select **SA-Shared-01-Remote**.
13. From the **Host** drop-down menu, select **sa-esxi-02.vclass.local**.
14. Leave all other fields at default value and click **OK**.

15. Click **Next**.

16. On the Configure Interfaces page, click the green plus sign to open the Add NSX Edge Interface dialog box, and configure the first of the two interfaces.

    a. In the **Name** text box, enter **`Uplink-Interface`**.

    b. For Type, leave **UpLink** selected.

    c. Click the **Connected To** > **Select** link.

    d. Click **Distributed Virtual Portgroup**.

    e. Click **pg-SA-Production** and click **OK**.

    f. Click the green plus sign.

    g. Enter **`172.20.11.3`** in the **Primary IP Address** text box.

    172.20.11.3 is the IP address for the NSX Edge uplink.

    h. Enter **`24`** in the **Subnet prefix length** text box.

    i. Leave all other settings at their default value and click **OK**.

17. Click the green plus sign to open the Add NSX Edge Interface dialog box, and configure the second interface.

    a. Enter **`Transit-Network`** in the **Name** text box.

    b. For Type, click **Internal**.

    c. Click the **Connected To** > **Select** link.

    d. Click **Transit-Network** and click **OK**.

    e. Click the green plus sign.

    f. Enter **`10.1.100.1`** in the **Primary IP Address** text box.

    10.1.100.1 is the IP address of the NSX Edge internal interface.

    g. Enter **`27`** in the **Subnet prefix length** text box.

    h. Leave all other fields at default value and click **OK**.

18. Compare the interface configurations to those in the table.

Name	IP Address	Subnet Prefix Length	Connected To
Uplink-Interface	172.20.11.3	24	pg-SA-Production
Transit-Network	10.1.100.1	27	Transit-Network

19. If any interface is not configured correctly, select that entry and click the pencil icon to edit the entry.

20. Click **Next**.

21. On the Default gateway settings page, select the **Configure Default Gateway** check box.

22. Verify that the vNIC selection is **Uplink-Interface.**

23. In the **Gateway IP** text box, enter **`172.20.11.10`**.

    172.20.11.10 is the IP address of the NSX Edge default gateway.

24. Leave all other settings at default value and click **Next**.

25. On the Firewall and HA page, select the **Configure Firewall default policy** check box.

26. For the Default Traffic Policy, click **Accept**.

    You must set Default Traffic Policy to **Accept** before proceeding.

    NOTE

    In this lab, you set the default traffic policy to be open so that the remaining labs will work. In the real world, you should be more selective about the traffic types allowed to flow through your edge gateway.

27. Leave all the other fields at the default values, and click **Next**.

28. On the Ready to Complete page, review the configuration report and click **Finish**.

29. Above the edge list, monitor the deployment to completion.

    The deployment is complete when 0 installations are active.

Task 3: Verify the NSX Edge Services Gateway Deployment

You verify the state of the deployed NSX Edge services gateway appliance by reviewing appliance configuration reports.

1. In the NSX Edges list, verify that the Perimeter Gateway entry is listed and that the type is NSX Edge.

2. Double-click the **Perimeter Gateway** entry to manage that object.

3. In the middle pane, click the **Manage** tab and click **Settings**.

4. In the Settings category panel, select **Interfaces**

5. In the Status column, verify that each configured interface has a green check mark.

6. In the settings category panel, select **Configuration**.

7. At the bottom of the middle pane, find the NSX Edge Appliances list.

   Q1. On what datastore is the perimeter gateway appliance deployed?

   Q2. On which host is the perimeter gateway appliance running?

8. Point to the vSphere Web Client **Home** icon and select **Hosts and Clusters**.
9. Expand the inventory tree of SA-Datacenter so that all the inventory for each cluster appears.
10. Click the vSphere Web Client **Refresh** icon.
11. In the inventory tree, select the perimeter gateway appliance in the SA-Management cluster.

    The appliance virtual machine name starts with Perimeter-Gateway and is followed by a number, for example, Perimeter-Gateway-0.
12. In the middle pane, click **Summary** to review the report.
13. Expand the **VM Hardware** section to review the hardware settings.

    Q3. How many vCPUs does the appliance have?

    Q4. How much total memory does the appliance have?

    Q5. What is the size of appliance hard disk 1?

    Q6. What is the size of appliance hard disk 2?

    Q7. How many network adapters does the appliance have?

    Q8. How many network adapters are connected to port groups?

Task 4: Configure Static Routes on the NSX Edge Services Gateway

You configure a static route that specifies the transit network interface on the distributed router as the next hop for traffic destined to the Web-Tier, App-Tier, or DB-Tier logical switch networks.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the Navigator pane, select **NSX Edges**.
3. In the edge list, double-click the **Perimeter Gateway** entry to manage that object.
4. In the middle pane, click **Manage** and click **Routing**.
5. In the Routing category panel, select **Static Routes**.
6. Click the green plus sign to open the Add Static Route dialog box.
7. In the **Network** text box, enter **`10.1.0.0/16`**.
8. 10.1.0.0/16 is the workload VM network.
9. In the **Next Hop** text box, enter **`10.1.100.2`**.

   This value is the distributed router interface on the Transit network.
10. From the **Interface** drop-down menu, select **Transit-Network**.
11. Leave all other settings at their default value and click **OK**.
12. Above the static routes list, click **Publish Changes** and wait for the update to complete.
13. Verify that the new route appears in the list and that Type appears as user.

Task 5: Configure Static Routes on the Distributed Router

You configure a static route that specifies the Transit-Network interface on the NSX Edge services gateway as the next hop for traffic destined to the Management network.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the Navigator pane, select **NSX Edges**.
3. In the edge list, double-click the **Distributed Router** entry to manage that object.
4. In the middle pane, click **Manage** and click **Routing**.
5. In the routing category panel, verify that **Static Routes** is selected.
6. Click the green plus sign to open the Add Static Route dialog box.
7. Enter **`172.20.10.0/24`** in the **Network** text box.

   172.20.10.0/24 is the student desktop network.

8. Enter **`10.1.100.1`** in the **Next Hop** text box.

   This address is the address of the perimeter gateway internal interface on Transit-Network.

9. From the **Interface** drop-down menu, select **Transit-Network**.
10. Leave all other settings at their default value and click **OK**.
11. Above the static routes list, click **Publish Changes** and wait for the update to complete.
12. Verify that the new route appears in the list and that Type appears as user.

Task 6: Test Connectivity Between an External Network and a Logical Switch Network

You use the static routes defined on the distributed router and the NSX Edge services gateway to test bidirectional communication over the transit network.

1. Open the web-sv-01a console window.
2. At the web-sv-01a command prompt, ping the student desktop system.

   ```
   ping 172.20.10.80
   ```

3. Verify that ICMP echo replies are received
4. Press Ctrl+C to stop the `ping` command.

   The `ping` test demonstrates the bidirectional connectivity between the logical switch network and the Management network for traffic that is initiated on the Web-Tier network. If the `ping` command does not receive the expected replies, ask your instructor for help.

5. In the browser window, press Ctrl+Alt to release the pointer.
6. Open a new browser tab, and browse to the web-sv-01a IP address.

   ```
   http://10.1.10.11
   ```

   The web-sv-01a webpage is displayed.

7. Browse to the web-sv-02a IP address.

   ```
   http://10.1.10.12
   ```

   The web-sv-02a webpage is displayed.

8. Close the browser tab that is used to browse the web servers.

   The `ping` and HTTP tests verify bidirectional connectivity between the Management and Web-Tier networks for connections initiated in either direction.

9. Minimize the browser window.

10. In the Command Prompt window on the student desktop, verify that the static routes enable bidirectional connectivity between the Management network and the App-Tier logical switch network.

    ```
    ping 10.1.20.11
    ```

11. Verify that the `ping` was successful.

12. Verify that the static routes enable bidirectional connectivity between the Management network and the DB-Tier logical switch network.

    ```
    ping 10.1.30.11
    ```

13. Verify that the `ping` was successful.

14. Leave the Command Prompt window open.

15. Restore the browser window, and click the **vSphere Web Client** tab.

Task 7: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. At the top of the vSphere Web Client, point to the **Home** icon and select **Networking & Security**.
2. In the browser window, leave the **vSphere Web Client** tab open.
3. Leave the web-sv-01a console window open.
4. On the student desktop, leave the Command Prompt window and MTPuTTY open.

Lab 7 Configuring and Testing Dynamic Routing on NSX Edge Appliances

Objective: Configure OSPF to establish bidirectional connectivity between the Management network and the Web-Tier, App-Tier, and DB-Tier logical switch networks

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Remove Static Routes from the Perimeter Gateway
3. Configure OSPF on the Perimeter Gateway
4. Redistribute the Perimeter Gateway Subnets
5. Remove Static Routes on the Distributed Router
6. Configure OSPF on the Distributed Router
7. Redistribute Distributed Router Internal Subnets
8. Troubleshoot Connectivity Between the Logical Switch Networks and the Management Network
9. Resolve the Connectivity Problem
10. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. In the task bar of the student desktop, click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
3. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
4. When prompted, select the **Use Windows session authentication** check box and click **Login**.
5. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.
6. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.

Task 2: Remove Static Routes from the Perimeter Gateway

You remove the static routes that you configured in lab 6 and use the Open Shortest Path First (OSPF) routing protocol to configure dynamic routing.

1. Minimize the browser window.
2. In the Command Prompt window on the student desktop, test bidirectional connectivity between the Management network and the Web-Tier logical switch network.

   ```
   ping 10.1.10.11
   ```

3. Verify that ICMP echo replies are received.

   If ICMP echo replies are not received, you might not have configured static routing when the NSX Edge services gateway was deployed in lab 6. Ask your instructor for help if you do not see the expected replies.

4. Leave the Command Prompt window open.

5. Restore the browser window.

6. In the Navigator pane, select **NSX Edges.**

7. In the edge list, double-click the **Perimeter Gateway** entry to manage that object.

8. In the middle pane, click **Manage** and click **Routing**.

9. In the routing category panel, select **Static Routes**.

10. In the static routes list, select the static route created lab 6, and click the red X to delete the entry.

11. Above the static routes list, click **Publish Changes**.

12. Minimize the browser window.

13. In the Command Prompt window on the student desktop, test bidirectional connectivity (which is not yet established) between the Management network and the Web-Tier logical switch network.

    ```
    ping 10.1.10.11
    ```

14. Verify that ICMP echo replies are not received.

    A `TTL expired in transit` message appears.

15. Leave the Command Prompt window open.

16. Restore the browser window.

Task 3: Configure OSPF on the Perimeter Gateway

You configure OSPF on the perimeter gateway so that the routes to the logical switch networks are learned from the distributed router over the transit network.

1. In Perimeter Gateway's Routing categories panel, select **Global Configuration**.

2. In the Dynamic Routing Configuration panel, click **Edit** to open the Edit Dynamic Routing Configuration dialog box.

    a. From the **Router ID** drop-down menu, select **Uplink-Interface - 172.20.11.3**.

    b. Click **OK**.

    c. On the top of the Global Configuration page, click **Publish Changes**.

3. In the Routing category panel, select **OSPF**.

4. In the OSPF Configuration panel, Click **Edit**.

5. In the OSPF Configuration dialog box, select the **Enable OSPF** check box, leave other settings as default value, and click **OK**.

6. Click **Publish Changes** at the top of the OSPF page.

7. In the **Area Definitions** panel, click the green plus sign to open the New Area Definition dialog box.

   a. Enter **829** in the **Area ID** text box.

   b. Leave all other settings at the default value and click **OK**.

8. Under Area to Interface Mapping, click the green plus sign at the bottom of the OSPF page to open the New Area to Interface Mapping dialog box.

9. Select **Transit-Network** from the drop-down menu.

10. Select **829** from the **Area** drop-down menu.

11. Leave all other fields at the default value and click **OK**.

12. At the top of the OSPF page, click **Publish Changes**.

Task 4: Redistribute the Perimeter Gateway Subnets

You configure which type of subnets are advertised by the perimeter gateway through OSPF.

1. In the Routing category panel, select **Route Redistribution**.

2. Under the Route Redistribution table, click the green plus sign at the bottom of the page to open the New Redistribution criteria dialog box.

3. Under Allow learning from, select the **Connected** check box.

4. Subnets that are connected to the perimeter gateway can be learned.

5. Leave all other settings at the default value and click **OK**.

6. Change the redistribution settings.

   a. On the right side of the Route Redistribution Status panel, click **Edit**.

   b. In the Change redistribution settings dialog box, select the **OSPF** check box to enable redistribution for OSPF.

   c. Click **OK**.

   d. In the Route Redistribution Status panel, verify that a green check mark appears next to OSPF at the top of the page.

7. At the top of the page, click **Publish Changes**.

Task 5: Remove Static Routes on the Distributed Router

You remove the static routes configured in an earlier lab in preparation to configure dynamic routing by using the OSPF routing protocol.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the Navigator pane, select **NSX Edges**.
3. In the edge list, double-click the **Distributed Router** entry to manage that object.
4. In the middle pane, click **Manage** and click **Routing**.
5. In the Routing category panel, select **Static Routes**.
6. In the static routes list, select the static route created in lab 6, and click the red X to delete the entry.
7. Above the static routes list, click **Publish Changes**.

Task 6: Configure OSPF on the Distributed Router

You configure OSPF on the distributed router.

1. In the Routing category panel, select **Global Configuration**.
2. On the right side of the Dynamic Routing Configuration panel, click **Edit**.
3. Select **Transit-Network - 10.1.100.2** from the **Router ID** drop-down menu in the Edit Dynamic Routing Configuration dialog box.

   This setting must be specified before OSPF can be configured.
4. Leave all other fields at their default value and click **OK**.
5. At the top of the Global Configuration page, click **Publish Changes**.
6. In the Routing category panel, select **OSPF**.
7. On the right side of the OSPF Configuration panel, click **Edit** to open the OSPF Configuration dialog box.
8. Select the **Enable OSPF** check box.
9. In the **Protocol Address** text box, enter **`10.1.100.3`**.
10. 10.1.100.3 is the protocol IP address for the distributed logical router OSPF configuration.
11. In the **Forwarding Address** text box, enter **`10.1.100.2`**.
12. 10.1.100.2 is the forwarding IP address for distributed logical router OSPF configuration.
13. Leave other fields at their default value and click **OK**.

14. In the Area Definitions panel, click the green plus sign to open the New Area Definition dialog box.

15. Enter **829** in the **Area ID** text box.

16. Leave all other fields at their default value and click **OK**.

17. In the Area to Interface Mapping panel, click the green plus sign to open the New Area to Interface Mapping dialog box.

18. Verify that the interface selection is **Transit-Network.**

19. Select **829** from the **Area** drop-down menu.

20. Leave all other fields at their default value and click **OK**.

21. At the top of the OSPF configuration page, click **Publish Changes**.

22. After the changes are published, verify that OSPF configuration status is Enabled.

Task 7: Redistribute Distributed Router Internal Subnets

You configure which type of subnets are advertised by the distributed router through OSPF.

1. In the Distributed Router's Routing category panel, select **Route Redistribution**.

2. In the Route Redistribution table, select the single entry that appears, click the pencil icon to open the Edit Redistribution criteria dialog box, and verify the settings.

   - Prefix Name: Any
   - Learner Protocol: OSPF
   - Allow Learning From: Connected
   - Action: Permit

3. Click **Cancel**.

   If the default route redistribution entry does not appear in the list or is not configured as specified, you must create a new route redistribution by clicking the green plus sign and configuring the criteria as specified in step 2.

Task 8: Troubleshoot Connectivity Between the Logical Switch Networks and the Management Network

You verify the OSPF configuration and troubleshoot connectivity between a logical switch network that is connected to the distributed router and the Management network.

1. Minimize the browser window.
2. In the Command Prompt window on the student desktop, test the bidirectional connectivity (which is not yet established) between the Management network and the Web-Tier logical switch network.

   ```
   ping 10.1.10.11
   ```

   10.1.10.11 is the IP address of the web-sv-01a virtual machine.
3. Verify that ICMP echo replies are not received.
4. Leave the Command Prompt window open.
5. Restore the browser window.
6. Verify the distributed router configuration, correcting it as necessary.
   a. In the routing category panel, select **Global Configuration**.
   b. In the Dynamic Routing Configuration panel, verify that the options are correctly configured.
      - Router ID: 10.1.100.2, the router ID for the distributed logical router
      - OSPF: Started, with a green check mark
   c. In the Routing category panel, select **Static Routes**.
   d. In the static routes table, verify that no static routes are defined.
   e. In the Routing category panel, select **OSPF**.
   f. In the OSPF Configuration panel, verify that the options are correctly set.
      - Status: Started
      - Protocol Address: 10.1.100.3, the protocol IP address for the distributed logical router OSPF configuration
      - Forwarding Address: 10.1.100.2, the forwarding IP address for distributed logical router OSPF configuration
   g. In the Area Definitions panel, verify that area 829 is defined with Normal for Type and None for Authentication.
   h. In the Area to Interface Mapping panel, verify that area 829 is mapped to Transit-Network.
   i. In the Routing category panel, select **Route Redistribution**.
   j. In the Route Redistribution Status panel, verify that a green check mark appears next to OSPF.

k. In the Route Redistribution table, verify that an entry exists with the correct criteria.

   - Learner: OSPF
   - From: Connected
   - Prefix: Any
   - Action: Permit

7. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
8. In the Navigator pane, select **NSX Edges**.
9. In the edge list, double-click the **Perimeter Gateway** entry to manage that object.
10. In the middle pane, click **Manage** and click **Routing**.
11. Verify the perimeter gateway configuration, correcting it as necessary.

    a. In the routing category panel, select **Global Configuration**.

    b. In the Dynamic Routing Configuration panel, verify that the options are correctly configured.

       - Router ID: 172.20.11.3, the router ID for the perimeter gateway
       - OSPF: Started, with a green check mark

    c. In the routing category panel, select **Static Routes**.

    d. In the static routes table, verify that no static routes are defined.

    e. In the routing category panel, select **OSPF**.

    f. At the top of the OSPF page, verify that the OSPF Status is Started.

    g. In the Area Definitions panel, verify that area 829 is defined with Normal for Type and None for Authentication.

    h. In the Area to Interface Mapping panel, verify that area 829 is mapped to Transit-Network.

    i. In the routing category panel, select **Route Redistribution**.

    j. In the Route Redistribution Status panel, verify that a green check mark appears next to OSPF.

    k. In the Route Redistribution table, verify that an entry exists with the correct criteria.

       - Learner: OSPF
       - From: Connected
       - Prefix: Any
       - Action: Permit

12. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.

13. In the Navigator pane, select **NSX Edges**.
14. In the edge list, double-click the **Distributed Router** entry.
15. In the middle pane, click the **Manage** tab and click **Settings**.
16. In the Settings category panel, select **Interfaces**.

Q1. Are the logical switch networks, Web-Tier, App-Tier, and DB-Tier, connected to distributed router interfaces?

17. On the **Manage** tab, click **Routing**.
18. In the routing category list, select **Static Routes**.

Q2. Are there subnets not directly connected that the distributed router should advertise?

19. In the routing category panel, select **Route Redistribution**.

Q3. Is the configured Route Redistribution entry sufficiently configured so that subnets known to the distributed router can be learned through OSPF?

20. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
21. In the Navigator pane, select **NSX Edges**.
22. In the edge list, double-click the **Perimeter Gateway** entry to manage that object.
23. In the middle pane, click the **Manage** tab and click **Settings**.
24. In the settings category panel, select **Interfaces**.

Q4. Is the Management network attached to the perimeter gateway?

25. On the **Manage** tab, click **Routing**.
26. In the routing category panel, select **Static Routes**.

Q5. Is the Management network identified by a static route?

27. In the routing category panel, select **Route Redistribution**.

Q6. Is the current route redistribution configured to allow the learning of static routes through OSPF?

Task 9: Resolve the Connectivity Problem

You configure the perimeter gateway with a static route to the Management network and configure OSPF to advertise static routes.

1. Verify that **Perimeter Gateway** appears in the Navigator pane.
2. Click **Manage** and click **Routing**.
3. In the Routing category panel, select **Static Routes**.
4. Click the green plus sign to open the Add Static Route dialog box.
5. In the **Network** text box, enter **`172.20.10.0/24`**.

   172.20.10.0/24 is the student desktop/Management network.
6. In the **Next Hop** text box, enter **`172.20.11.10`**.

   This address is the address of the RAS router on the Production network.
7. From the **Interface** drop-down menu, select **Uplink-Interface**.
8. Leave all other settings at default value and click **OK**.
9. Click **Publish Changes**.
10. In the routing category panel, select **Route Redistribution**.
11. In the Route Redistribution table, select the single entry that appears, and click the pencil icon to open the Edit Redistribution criteria dialog box.
12. Under Allow learning from, select the **Static Routes** check box.
13. Click **OK**.
14. At the top of the Route Redistribution page, click **Publish Changes**.

    The configuration change instructs the perimeter gateway to allow learning of both connected subnets and static routes through OSPF. The distributed router receives a route to the Management network from the perimeter gateway with a next hop of the perimeter gateway interface on the transit network.
15. Minimize the browser window.
16. In the Command Prompt window on the student desktop, test bidirectional connectivity between the Management network and the Web-Tier logical switch network.

    ```
    ping 10.1.10.11
    ```

    10.1.10.11 is the IP address of the web-sv-01a virtual machine.
17. Verify that the ping is successful.

18. If the ping is not successful (ICMP replies are not received), wait for about 60 seconds and ping again until the ICMP replies are received.

19. Run `ping` tests to verify connectivity between the Management network and the App-Tier and DB-Tier logical switch networks.

    ```
    ping 10.1.20.11
    ```

    ```
    ping 10.1.30.11
    ```

    10.1.20.11 is the IP address of the app-sv-01a virtual machine. 10.1.30.11 is the IP address of the db-sv-01a virtual machine.

    Both pings should be successful.

20. Leave the Command Prompt window open.

21. Restore the browser window.

Task 10: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the browser window, leave the **vSphere Web Client** tab open.
3. Leave the web-sv-01a console window open.
4. On the student desktop, leave the Command Prompt window open.

Lab 8 Configuring Equal-Cost Multipathing

Objective: Configure ECMP to load-balance traffic in the north-south direction

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Deploy an Additional NSX Edge Services Gateway
3. Configure Routing for Perimeter Gateway - ECMP
4. Configure a Static Route on Perimeter Gateway - ECMP
5. Configure Route Redistribution for Perimeter Gateway - ECMP
6. Verify the Relationship Between the Distributed Logical Router Routing Table and the Neighbor
7. Enable ECMP
8. Disable ECMP, and Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. In the task bar of the student desktop, click the **Command Prompt** shortcut in the task bar.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
3. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
4. When prompted, select the **Use Windows session authentication** check box and click **Login**.

Task 2: Deploy an Additional NSX Edge Services Gateway

You configure and deploy an additional NSX Edge services gateway to demonstrate the equal-cost multipath (ECMP) capability of the distributed logical router.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the Navigator pane, select **NSX Edges.**
3. In the middle pane, click the green plus sign to open the New NSX Edge dialog box.
4. On the Name and description page, leave **Edge Services Gateway** selected.
5. In the **Name** text box, enter **`Perimeter-Gateway-ECMP`** and click **Next**.
6. On the Settings page, leave **User Name** as admin, and enter **`VMware1!VMware1!`** in the **password** text box and the **Confirm password** text box.
7. Select the **Enable SSH access** check box and click **Next**.
8. On the Configure deployment page, verify that **SA-Datacenter** is selected.
9. Verify that the Appliance Size selection is **Compact**.
10. Under NSX Edge Appliances, click the green plus sign to open the Add NSX Edge Appliance dialog box.
11. From the **Cluster/Resource Pool** drop-down menu, select **SA-Management**.
12. From the **Datastore** drop-down menu, select **SA-Shared-01-Remote**.
13. From the **Host** drop-down menu, select **sa-esxi-01.vclass.local**.
14. Leave all other fields at their default value and click **OK**.
15. Click **Next**.

16. On the Configure Interfaces page, click the green plus sign to open the Add NSX Edge Interface dialog box and configure the first of the two interfaces.

    a. In the **Name** text box, enter `Uplink-Interface`.

    b. For Type, leave **UpLink** selected.

    c. Click the **Connected To > Select** link.

    d. Click **Distributed Virtual Portgroup**.

    e. Click **pg-SA-Production** and click **OK**.

    f. Click the green plus sign.

    g. In the **Primary IP Address** text box, enter `172.20.11.4`.

       172.20.11.4 is the IP address for the Perimeter Gateway - ECMP Edge uplink.

    h. Enter `24` in the **Subnet prefix length** text box.

    i. Leave all other settings at their default value and click **OK**.

17. Click the green plus sign to open the Add NSX Edge Interface dialog box and configure the second interface.

    a. In the **Name** text box, enter `Transit-Network`.

    b. For Type, click **Internal**.

    c. Click the **Connected To > Select** link.

    d. Under Logical Switch, click **Transit-Network** and click **OK**.

    e. Click the green plus sign

    f. In the **Primary IP Address** text box, enter `10.1.100.4`.

       10.1.100.4 is the IP address for the Perimeter Gateway - ECMP Edge internal interface.

    g. Enter `27` in the **Subnet prefix length** text box.

    h. Leave all other fields at their default value and click **OK**.

18. Compare the interface configurations to those in the table.

Name	IP Address	Subnet Prefix Length	Connected To
Uplink-Interface	172.20.11.4	24	pg-SA-Production
Transit-Network	10.1.100.4	27	Transit-Network

19. If any interface is not configured correctly, select that entry and click the pencil icon to edit the entry.

20. Click **Next**.

21. On the Default gateway settings page, select the **Configure Default Gateway** check box.

22. Verify that the vNIC selection is **Uplink-Interface.**

23. In the **Gateway IP** text box, enter **`172.20.11.10`**.

    172.20.11.10 is the IP address of the NSX Edge default gateway.

24. Leave all other settings at their default value and click **Next**.

25. On the Firewall and HA page, select the **Configure Firewall default policy** check box.

26. For the Default Traffic Policy, click **Accept**.

    You must accept the default traffic policy before proceeding.

27. Leave all the other fields at their default value and click **Next**.

28. On the Ready to Complete page, review the configuration report and click **Finish**.

29. Above the edge list, monitor the deployment to completion.

    The deployment is complete when 0 installations are active.

Task 3: Configure Routing for Perimeter Gateway - ECMP

You configure OSPF routing and create a static route on the Perimeter Gateway - ECMP edge router.

1. Double-click **Perimeter-Gateway-ECMP** in the middle pane.

2. Click the **Manage** tab and click **Routing**.

3. In the Routing categories panel, select **Global Configuration**.

4. In the Dynamic Routing Configuration panel, click **Edit** to open the Edit Dynamic Routing Configuration dialog box.

5. Select **Uplink-Interface - 172.20.11.4** from the **Router ID** drop-down menu.

6. Click **OK**.

7. At the top of the Global Configuration page, click **Publish Changes**.

8. In the Routing category panel, select **OSPF**.

9. To the right side of OSPF Configuration, click **Edit**.

10. In the OSPF Configuration dialog box, select the **Enable OSPF** check box and click **OK**.

11. Click **Publish Changes** at the top of the OSPF page.

12. Under Area Definitions, click the green plus sign to open the New Area Definition dialog box.
13. Enter **`829`** in the **Area ID** text box.
14. Leave all other settings at their default value and click **OK**.
15. Under Area Interface Mapping, click the green plus sign at the bottom of the OSPF page to open the New Area to Interface Mapping dialog box.
16. Select **Transit-Network** from the drop-down menu.
17. Select **829** from the **Area** drop-down menu.
18. Leave all other fields at their default value and click **OK**.
19. At the top of the OSPF page, click **Publish Changes**.

Task 4: Configure a Static Route on Perimeter Gateway - ECMP

You configure the perimeter gateway with a static route to the Management network.

1. In the Routing category panel, select **Static Routes**.
2. Click the green plus sign to open the Add Static Route dialog box.
3. In the **Network** text box, enter **`172.20.10.0/24`**.

   172.20.10.0/24 the student desktop/Management network address.
4. In the **Next Hop** text box, enter **`172.20.11.10`**.

   This address is the address of the RAS router on the Production network.
5. From the **Interface** drop-down menu, select **Uplink-Interface**.
6. Leave all other settings at their default value and click **OK**.
7. Click **Publish Changes**.

Task 5: Configure Route Redistribution for Perimeter Gateway - ECMP

You configure which type of subnets are advertised by the perimeter gateway through OSPF.

1. In the Routing category panel, select **Route Redistribution**.
2. Under the Route Redistribution table, click the green plus sign at the bottom of the page to open the New Redistribution criteria dialog box.
3. Under Allow learning from, select the **Connected** and the **Static routes** check boxes.
4. Leave all other settings at their default value and click **OK**.
5. In the Route Redistribution Status panel, determine if a green check mark appears next to OSPF at the top of the page.

   You should not yet see the green check mark next to OSPF.
6. If a green check mark does not appear, change the redistribution setting.
   a. On the right side of the Route Redistribution Status panel, click **Edit**.
   b. In the Change redistribution settings dialog box, select the **OSPF** check box.
   c. Click **OK**.
   d. In the Route Redistribution Status panel, verify that a green check mark appears next to OSPF at the top of the page.
7. At the top of the page, click **Publish Changes**.

Task 6: Verify the Relationship Between the Distributed Logical Router Routing Table and the Neighbor

You verify the OSPF configuration and routing table on the distributed logical router.

1. Point to the vSphere Web Client **Home** icon and select **Hosts and Clusters**.
2. Expand the inventory of SA-Datacenter and select the **Distributed Router-0** VM.
3. Open the virtual machine console for Distributed Router-0.
   a. Click the **Summary** tab.
   b. Click the console thumbnail image.
   c. If prompted to log in, log in as admin and with the password VMware1!VMware1!.
4. Run the `show ip ospf neighbor` command, and verify that the logical router has formed adjacency with both of the edge routers.
5. Run the `show ip route` command to display the routing table.

   The distributed logical router adds only one edge router as the next hop to reach the Management network, because ECMP is not enabled.

Task 7: Enable ECMP

You enable ECMP on the distributed logical router.

1. Click the **vSphere Web Client** tab in the browser.
2. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
3. Select **NSX Edges** in the Navigator pane.
4. Double-click the **Distributed Router** instance in the middle pane.
5. Click the **Manage** tab and click **Routing**.
6. Select **Global Configuration.**
7. Under **Routing Configuratio**n, click **Start** next to **ECMP**.
8. Click **Publish Changes** at the top of the Routing Configuration page.
9. Click the **Distributed Router-0** console tab in browser.
10. Run the `show ip ospf neighbor` command and verify that the logical router has still formed adjacency with both the edge routers.
11. Run the `show ip route command` to display the routing table.

    An entry for each edge router exists as the next hop toward the Management network. The distributed logical router can now use the two paths to distribute the traffic load.

    NOTE

    You might need to wait for 30 seconds for the command to display the expected output.

Task 8: Disable ECMP, and Clean Up for the Next Lab

You disable ECMP on the distributed logical router and prepare for the next lab.

1. Click the **vSphere Web Client** tab in browser.
2. Ensure that you are at the Distributed Router's Global Configuration view.
   a. Point to the **Home** icon and select **Networking & Security**.
   b. Select **NSX Edges** and double-click **Distributed Router**.
   c. Click **Manager** and click **Routing**.
   d. Select **Global Configuration**.
3. Under **Routing Configuration**, click **Stop** next to **ECMP**.
4. Click **Publish Changes** at the top of the Routing Configuration page.
5. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
6. In the Navigator pane, select **NSX Edges**.
7. Select **Perimeter Gateway - ECMP**, and click the red X to delete the additional edge router.
8. When prompted by the Delete NSX Edge warning message, click **Yes** to confirm the deletion.
9. In the browser window, leave the **vSphere Web Client** tab open.
10. In the browser window, close the **Distributed Router-0** console tab.

Lab 9 Configuring NSX Edge High Availability

Objective: Configure high availability, and use the NSX Edge command line to determine the current HA status and view heartbeat traffic

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Configure NSX Edge High Availability
3. Examine the High Availability Service Status and Heartbeat
4. Force a Failover Condition
5. Restore the Failed Node
6. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. In the task bar of the student desktop, click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the MTPuTTY window is not open on the student desktop, open the MTPuTTY window.
   a. In the task bar of the student desktop, click the **MTPuTTY** shortcut.
   b. In the MTPuTTY window, click **Server** and select **Add server**.
   c. In the **Server name** text box, enter **`172.20.11.3`**.

      172.20.11.3 is the perimeter gateway IP address.

   d. Select **SSH** as the protocol.
   e. In the **Display name** text box, enter **`Perimeter-Gateway`**.
   f. Click **OK**.
   g. In the left pane of MTPuTTY, double-click the **Perimeter Gateway** session that you added.
   h. If prompted to confirm a PuTTY security alert, click **Yes**.
   i. Log in as admin and enter the password **`VMware1!VMware1!`**.
3. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
4. If you are not logged in to vSphere Web Client, click the **vSphere Site-A vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
5. When prompted, select the **Use Windows session authentication** check box and click **Login**.
6. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in Internet Explorer.
7. On the vSphere Web Client **Home** tab, click the **Networking & Security** icon.

Task 2: Configure NSX Edge High Availability

You configure the perimeter gateway for high availability.

1. In the Navigator pane, select **NSX Edges**.
2. In the edge list, double-click the **Perimeter Gateway** entry to manage that object.
3. In the middle pane, click the **Manage** tab and click **Settings**.
4. In the Settings category panel, select **Configuration**.
5. On the Configuration page, in the HA Configuration panel, determine the current high availability status of the edge.

   The status is Disabled.
6. In the HA Configuration panel, click the **Change** link to configure and enable high availability.
7. In the Change HA configuration dialog box, configure the settings.
   a. Click **Enable**.
   b. In the two text boxes for configuring management IP addresses, enter the IP addresses in Classless Inter-Domain Routing format.
      - 192.168.222.1/30
      - 192.168.222.2/30
   c. Leave all the remaining settings at their default value and click **OK**.
8. Wait for the high availability configuration update to finish, and verify that the HA status in the HA Configuration panel is Enabled.
9. Point to the vSphere Web Client **Home** icon and select **Hosts and Clusters**.
10. Expand the Hosts and Clusters inventory tree of SA-Datacenter so that the SA-Management Cluster inventory is visible.
11. In the SA-Management Cluster inventory, find all virtual machines with names starting with Perimeter-Gateway.

12. Select each perimeter gateway virtual machine and review the **Summary** tab.

    Q1. How many instances of the perimeter gateway did you find?

    Q2. Which host is Perimeter Gateway-0 running on?

    Q3. Which host is Perimeter Gateway-1 running on?

    Q4. Are the NSX Edge instances running on different hosts?

13. Remain in the Hosts and Clusters inventory.

Task 3: Examine the High Availability Service Status and Heartbeat

You use command-line tools to query the high availability service status and examine the heartbeat network traffic.

1. Minimize the Internet Explorer window.
2. In the saved Perimeter Gateway MTPuTTY session window, run the command to show the status of the high availability service.

   ```
   show service highavailability
   ```

3. Examine the command output.

   This command uses the generic vshield-edge name for the NSX Edge instances. See the vCenter Server inventory for which gateway has a trailing -0 or -1 to associate what the command is showing with the perimeter gateway nodes. In the command output, look for `Highavailibility Healthcheck status` for `This unit` or `Peer unit`.

   Q1. Which of the perimeter gateway nodes is active?

   Q2. Are both peer nodes in good health?

   Q3. Are the file synchronization and connection synchronization services necessary for failover running?

4. At the command prompt, display the high availability heartbeat packets captured on the transit network interface.

   ```
   debug packet display interface vNic_1
          net_192.168.222.0_mask_255.255.255.252
   ```

5. Examine the exchange and verify that the two high availability nodes are actively communicating status to each other.

   You should see packets exchanged between the following IP addresses:

   - 192.168.222.1
   - 192.168.222.2

6. Keep the traffic capture running, and restore the browser window.

Task 4: Force a Failover Condition

You power off the high availability active node to force a failover to the standby node.

1. In the Hosts and Clusters inventory tree, select **Perimeter Gateway-0**, or whichever of the two perimeter gateway nodes is listed as active in task 3.
2. Right-click **Perimeter Gateway-0** and select **Power** > **Shut Down Guest OS**.
3. Click **Yes** when prompted to confirm.
4. Monitor the appliance shutdown until the task appears as complete in the Recent Tasks pane and a running indicator icon no longer appears on the virtual machine in the cluster inventory.
5. Minimize the browser window.
6. Close the MTPuTTY window.

   The SSH session to the perimeter gateway is terminated because the virtual machine is shut down.

7. In the MTPuTTY application, double-click the saved **Perimeter Gateway** session to connect to the perimeter gateway.
8. Log in as admin and enter the password **`VMware1!VMware1!`**.
9. Show the status of the high availability.

   ```
   show service highavailability
   ```

10. Examine the command output.

    In the content of the command output, look for the `highavailibility` unit name to determine the active node name.

    Q1. Which of the perimeter gateway nodes is active?

    Q2. Are both peer nodes in good health?

    Q3. Are services necessary for failover running, specifically file synchronization and connection synchronization?

    Q4. Has a failover occurred?

11. At the command prompt, display the high availability heartbeat packets captured on the transit network interface.

    ```
    debug packet display interface vNic_1
           net_192.168.222.0_mask_255.255.255.252
    ```

12. Examine the packet exchange, and verify that only the active node is communicating heartbeat information and is receiving no replies from the peer node.

13. Keep the traffic capture running, and restore the browser window.

Task 5: Restore the Failed Node

You power on the stopped node to restore the high availability pair. And you use command-line tools to examine changes in the high availability service configuration.

1. In the Hosts and Clusters inventory, right-click the powered-off perimeter gateway and select **Power** > **Power On**.

2. Minimize the browser window.

3. In the MTPuTTY window, monitor the packet capture until you observe both nodes communicating heartbeat information again.

4. Press Ctrl+C to stop the packet capture.

5. Show the status of the high availability service.

    ```
    show service highavailability
    ```

6. Examine the command output.

   In the content of the command output, look for the `highavailibility` unit name to determine the active node name.

   Q1. Which of the perimeter gateway nodes is active?

   Q2. Are both peer nodes in good health?

   Q3. Are services necessary for failover running, specifically file synchronization and connection synchronization?

   Q4. Has a failback occurred?

Task 6: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Leave the MTPuTTY window open.
2. Leave the Command Prompt window open.
3. Restore the browser window.
4. Point to the vSphere Web Client **Home** icon and select **Networking**.
5. In the browser window, leave the **vSphere Web Client** tab open.
6. Leave the web-sv-01a console window open.

Lab 10 Configuring Layer 2 Bridging

Objective: Configure L2 bridging in the software

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Create a Port Group on the Distributed Switch for L2 Bridging
3. Move the Two Web Servers to the Host That Runs the Distributed Logical Router Control VM
4. Examine the Network Connectivity Between Web VMs and Resolve the Problem
5. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
2. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
3. When prompted, select the **Use Windows session authentication** check box and click **Login**.

Task 2: Create a Port Group on the Distributed Switch for L2 Bridging

You create a port group that is used for setting up an L2 bridge.

1. Point to the vSphere Web Client **Home** icon and select **Networking**.
2. In the Navigator pane, select **dvs-SA-Datacenter**.
3. In the middle pane, click **Actions** and select **Distributed Port Group** > **New Distributed Port Group**.

   The New Distributed Port Group window appears.
4. On the Select name and location page, enter **`L2PG`** in the **Name** text box and click **Next**.
5. On the Configure settings page, from the **VLAN type** drop-down menu, select **VLAN** and enter **`10`** as the VLAN ID.

   NOTE

   In the lab environment, the physical network is not configured to support VLAN 10. You use a dummy VLAN ID of 10 because setting up bridging requires the port group to be configured with a VLAN ID.
6. Click **Next**.
7. Click **Finish** on the Ready to Complete page.
8. Point to the **Home** icon and select **VMs and Templates**.
9. Select the **web-sv-02a** VM in the Navigator pane, and click **Actions** in the middle pane.
10. Select **Edit Settings**.
11. In the VMs Edit Settings dialog box, select **L2PG (dvs-SA-datacenter)** port group from the **Network Adapter 1** drop-down menu and click **OK**.

    You might have to select **Show more networks** to display the port group that you need.
12. Click **OK** to close the Edit Settings window.

Task 3: Move the Two Web Servers to the Host That Runs the Distributed Logical Router Control VM

You move the web-sv-01a and web-sv-02a virtual machines to the ESXi host running the distributed logical router control VM.

This task is not required in production environments. This task is performed in the lab because the physical network is not configured to support VLAN 10.

1. Select the **Distributed Router-0** VM in the Navigator pane.
2. Click the **Summary** tab in the middle pane.
3. Identify the ESXi host on which the Distributed Router-0 VM is running, and record the host name. __________
4. Select the **web-sv-01a** virtual machine in the Navigator pane.
5. Click **Actions** in the middle pane and select **Migrate**.
6. On the Select the migration type page, leave **Change compute resource only** selected and click **Next**.
7. On the Select a compute resource page, select the ESXi host where the Distributed Router-0 VM resides, which you recorded in step 3.
8. Click **Next**.
9. On the Select Network page, click **Next**.
10. On the Select vMotion priority page, click **Next**.
11. Click **Finish**.
12. Repeat steps 4 through 11 for web-sv-02a.

Task 4: Examine the Network Connectivity Between Web VMs and Resolve the Problem

You verify whether the Web VMs can communicate with each other. You fix the problem if they cannot communicate.

1. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.

2. Start a `ping` session to the web-sv-02a VM window.

```
ping 10.1.10.12
```

Q1. Does ping work?

3. Press Ctrl+C to stop the ping.
4. Return to the **vSphere Web Client** tab in browser window.
5. Point to the **Home** icon and select **Networking & Security**.
6. Select **NSX Edges** in the Navigator pane.
7. Double-click the **Distributed Router** instance in the middle pane.
8. Click the **Manage** tab and click **Bridging**.
9. Click the green plus sign under bridging.
10. In the Add Bridge dialog box, enter **`L2Bridge`** in the **Name** row.
11. Click the **Logical Switch** icon in the Logical Switches row and select **Web-Tier**.
12. Click **OK**.
13. Click the network icon in the Distributed Port Group row and select **L2PG**.
14. Click **OK**.
15. Click **Publish Changes** on the **Manage** tab.
16. Click the **web-sv-01a** VM console tab in the browser window.
17. Start a `ping` request to web-sv-02a.

```
ping 10.1.10.12
```

Q2. Is the ping to web-sv-02a successful?

18. Press Ctrl+C to stop the ping.

Task 5: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Click the **vSphere Web Client** tab in the browser.
2. Ensure that you are on the bridge instance view.
   a. Point to the **Home** icon and select **Networking & Security**.
   b. Select **NSX Edges** and double-click **Distributed Router**.
   c. Click the **Manage** tab and click **Bridging**.
3. Select the bridge instance, and click the red X to delete the bridge instance.
4. Click **Publish Changes**.
5. Point to the **Home** icon and select **VMs and Templates**.
6. Select the **web-sv-02a** VM in the Navigator pane.
7. Click **Actions** and select **Edit Settings**.
8. In the web-sv-02a Edit Settings dialog box, select the logical switch for Web-Tier from the **Network Adapter 1** drop-down menu.

   You might have to select **Show more networks** to display the port group that you need.
9. Click **OK** to close the Select Network window**.**
10. Click **OK** to close the Edit Settings window.
11. Migrate the web-sv-01a and web-sv-02a virtual machines back to the Compute cluster.
    a. In the Navigator pane, select **Hosts and Clusters**.
    b. From Management and Edge cluster, select the **web-sv-01a** VM and drop it to the Compute cluster.
    c. On the Select the migration type page, click **Change compute resource only** and click **Next**.
    d. On the Select a compute resource page, select **sa-esxi-04.vclass.local** in the Compute cluster and click **Next**.
    e. On the select network page, click **Next**.
    f. On the Select vMotion priority page, click **Next**.
    g. On the Ready to complete page, click **Finish**.
    h. Repeat steps a through g for web-sv-02a.
12. Point to the **Home** icon and select **Networking & Security**.

Lab 11 Configuring and Testing NAT on an NSX Edge Services Gateway

Objective: Use destination NAT and source NAT rules to establish a one-to-one relationship between the IP address of a web server on an internal subnet and an IP address in an externally accessible subnet

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Verify Untranslated Packet Addressing
3. Configure an Additional IP Address on the Uplink Interface of the Perimeter Gateway
4. Configure a Destination NAT Rule
5. Use the Destination NAT to Test Connectivity
6. Verify Untranslated Packet Addressing Before Defining a Source NAT Rule
7. Configure a Source NAT Rule
8. Use the Source NAT to Test Connectivity
9. Configure a Destination NAT Rule for web-sv-02a
10. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. On the student desktop, double-click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
3. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
4. When prompted, select the **Use Windows session authentication** check box and click **Login**.
5. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.
6. On the vSphere Web Client Home page, click **Networking & Security**.

Task 2: Verify Untranslated Packet Addressing

You use the packet capture capabilities of NSX Edge to verify source and destination addressing of packets that are exchanged by the student desktop system and the web-sv-01a web server.

1. Minimize the browser window.
2. In the task bar of the student desktop, click the **MTPuTTY** shortcut.
3. In the left pane of MTPuTTY, double-click the **Perimeter Gateway** session that you added.
4. Log in as admin and enter the password **`VMware1!VMware1!`**.
5. If you cannot log in because SSH access was not enabled during the deployment of the NSX Edge instance, or if the password was entered incorrectly, change the CLI credentials.

   a. Restore the browser window.

   b. In the Navigator pane, select **NSX Edges**.

   c. From the edge list, select **Perimeter Gateway**, and select **Change CLI Credentials** from the **Actions** drop-down menu.

   d. In the Change CLI credentials, enter **`VMware1!VMware1!`** in the **Password** and the **Retype Password** text boxes.

   e. Verify that the **Enable SSH Access** check box is selected and click **OK**.

   f. Restart this task by returning to step 1.

6. Begin capturing HTTP traffic on the uplink interface.

   All commands are case-sensitive.

   ```
   debug packet display interface vNic_0 port_80
   ```

   Include the `port_80` filter as the last argument of the command. The filter expression must be expressed with underscore characters where spaces might normally appear.

7. Leave the traffic capture running in the MTPuTTY window, and restore the browser window.
8. Open a new browser tab and enter **`http://10.1.10.11`** to browse to the web-sv-01a web server.

   You should be able to reach the web server page.

9. After the webpage is displayed, go to http://172.20.11.5 and verify that no response is received.

   172.20.11.5 is the network address translation (NAT) IP address that you will associate with the web-sv-01a virtual machine.

10. After the browser reports that the page cannot be displayed, close the browser tab and minimize the browser window.

11. In the MTPuTTY window, examine the packets that are captured to determine source and destination addressing format.

    Packet addressing is always reported in the following format:

    ```
    time protocol source-address.source-port > destination-address:
    destination-port
    ```

12. In the packet capture output, examine the addressing of each packet and verify that the correct addresses are involved in the exchange.

    - 172.20.10.80 - Student Desktop
    - 10.1.10.11 - web-sv-01

    Q1. In the packet capture, do you observe any packets exchanged between the student desktop system and the NAT IP address (172.20.11.5)?

13. Leave the packet capture running in the MTPuTTY window.
14. Restore the browser window.

Task 3: Configure an Additional IP Address on the Uplink Interface of the Perimeter Gateway

You configure a secondary IP address to the uplink interface of the NSX Edge perimeter gateway. This IP address is used for creating the NAT rule.

1. In the Navigator pane, select **NSX Edges**.
2. In the edge list, double-click the **Perimeter Gateway** entry to manage that object.
3. In the middle pane, click the **Manage** tab and click **Settings**.
4. In the Settings category panel, select **Interfaces**.
5. In the interfaces list, select the **vNIC# 0** entry that is associated with Uplink-Interface, and click the pencil icon.

   The Edit NSX Edge Interface dialog box appears.

6. Under Configure Subnets, select the existing IP address and click the pencil icon.
7. In the **Secondary IP address** text box, enter **`172.20.11.5`**.

   172.20.11.5 is the NAT IP address.

8. Click **OK** to commit the interface changes.
9. In the interfaces list, verify that the configured primary and secondary IP addresses for vNIC# 0 appear.

   You can click **Show All** to expand the IP address view.

Task 4: Configure a Destination NAT Rule

You create a destination NAT (DNAT) rule for translating the NAT IP address 1 to the IP address of web-sv-01a.

A DNAT rule can be assigned to any interface. You can assign destination NAT rules to only the interface that receives the network traffic to be translated, such as the uplink interface.

1. Under the **Manage** tab, click **NAT**.
2. Above the NAT rules list, click the green plus sign and select **Add DNAT Rule**.
3. In the Add DNAT Rule dialog box, add the destination NAT rule.
   a. From the **Applied On** drop-down menu, select **Uplink-Interface**.
   b. In the **Original Destination IP/Range** text box, enter **`172.20.11.5`**.
   c. In the **Translated IP/Range** text box, enter **`10.1.10.11`**.

      This address is the address of the web-sv-01a web server virtual machine that is attached to the Web-Tier logical switch network. The Web-Tier network is accessible from the perimeter gateway through an OSPF-learned route that has a next hop of Application Edge router on the transport network.

   d. Verify that the **Enabled** check box is selected.
   e. Leave all other settings at the default value and click **OK**.
4. Above the NAT rules list, click **Publish Changes**.
5. Wait for the update to complete, and verify that the new destination NAT rule appears in the list with a Rule Type of USER.

Task 5: Use the Destination NAT to Test Connectivity

You use the packet display capability of the NSX Edge services gateway command line to verify that the DNAT rule works as expected.

1. Open a new browser tab and go to http://172.20.11.5 to browse the web-sv-01a web server by using the destination NAT address.
2. After the webpage is displayed, keep the web server tab open and minimize the browser window.

3. In the MTPuTTY window, determine packet addressing and verify that the correct two IP addresses are involved in the exchange.

   - 172.20.10.80

     This address is the IP address of the student desktop.

   - 172.20.11.5

     This address is the destination NAT original address. For packets sent to this address, the destination was transformed from NAT address 1 to web-sv-01a's IP before being forwarded by NSX Edge. For response packets sent from the web server, the source address was translated so that the packets appear as if originating from the destination NAT address to maintain the integrity of the client-server connection.

4. Press Ctrl+C to stop the packet capture.

5. Begin capturing packets on Transit-Network.

   ```
   debug packet display interface vNic_1 port_80
   ```

6. Restore the browser window, and click the page refresh icon to reload the web server page (http://172.20.11.5).

7. After the webpage is displayed, close the browser tab and minimize the browser window.

8. In the MTPuTTY window, determine packet addressing and verify that the correct two IP addresses are involved in the exchange.

   - 172.20.10.80

   - 10.1.10.11

     This address is the destination NAT translated address of the web-sv-01a web server. The packets captured on the transit network are forwarded from the perimeter gateway to the distributed router with the destination address translated.

9. Press Ctrl+C to stop the packet capture, and leave the MTPuTTY window open.

10. Review the tests performed so far in this lab.

    Q1. If response traffic was not translated based on the destination NAT mapping, what source address would the packets have when received by the student desktop?

    Q2. For a TCP connection being established from student desktop to destination NAT IP for web-sv-01a, would the student desktop associate response packets from web-sv-01a with that connection?

Task 6: Verify Untranslated Packet Addressing Before Defining a Source NAT Rule

You verify the source and destination address of packets exchanged between the student desktop and the web-sv-01a web server virtual machine before applying a source NAT.

1. In the MTPuTTY window, begin capturing ICMP packets on the uplink interface.

   ```
   debug packet display interface vNic_0 icmp
   ```

2. Leave the packet capture running, and restore the web-sv-01a console window from the Windows task bar.

3. At the web-sv-01a command prompt, ping the student desktop system.

   ```
   ping 172.20.10.80
   ```

4. After at least one ICMP echo request and echo reply are reported, press Ctrl+C to stop the `ping` command.

5. Press Ctrl+Alt to release the pointer, and minimize the browser window.

6. In the MTPuTTY window, determine the source and destination addressing, and verify that the correct two IP addresses are involved in the ICMP exchange.

   - 172.20.10.80
   - 10.1.10.11

     This address is the untranslated IP address of the web-sv-01a web server virtual machine.

   The captured exchange shows that the web-sv-01a web server IP address is unaffected by the destination NAT rule when traffic is initiated from that address. The original web-sv-01a web server IP address is maintained as the packets leave the perimeter gateway in transit to the student desktop system.

7. Restore the browser window.

8. Click the **vSphere Web Client** tab.

Task 7: Configure a Source NAT Rule

You create a source NAT (SNAT) rule to translate the IP address of web-v-01a to NAT IP address 1 for outgoing connections.

An SNAT rule can be assigned to any interface. You can assign SNAT rules to the interface that connects to the translated network but not to the interface that received the original packet.

1. Verify that **Perimeter Gateway** appears in the Navigator pane.

2. Click the **Manage** tab and click the **NAT** tab.

3. Above the NAT rules list, click the green plus sign and select **Add SNAT Rule**.

4. In the Add SNAT Rule dialog box, configure the original and the translated source IP address.

   a. From the **Applied On** drop-down menu, select **Uplink-Interface**.

   b. In the **Original Source IP/Range** text box, enter **`10.1.10.11`**.

      10.1.10.11 is the IP address of the web-sv-01a virtual machine.

   c. In the **Translated Source IP/Range** text box, enter **`172.20.11.5`**.

      This address is the translated source IP address.

   d. Ensure that the **Enabled** check box is selected.

   e. Leave all other fields at their default value and click **OK**.

5. Above the NAT rules list, click **Publish Changes**.

Task 8: Use the Source NAT to Test Connectivity

Packets sent from the web-sv-01a web server virtual machine appear as originating from the perimeter gateway's external subnet.

1. Restore the web-sv-01a console window from the Windows task bar.

2. At the web-sv-01a command prompt, ping the student desktop system.

   ```
   ping 172.20.10.80
   ```

3. After at least one ICMP request and reply have been reported, press Ctrl+C to stop the `ping` command.

4. Press Ctrl+Alt to release the pointer and switch to the MTPuTTY window.

5. In the MTPuTTY window, determine source and destination addressing and verify that the correct two IP addresses are involved in the ICMP exchange.

   - 172.20.10.80
   - 172.20.11.5

     This address is the translated IP address of the web-sv-01a web server virtual machine.

6. In the MTPuTTY window, press Ctrl+C to stop the packet capture.

7. Restore the browser window.

8. Click the **vSphere Web Client** tab.

Task 9: Configure a Destination NAT Rule for web-sv-02a

You configure a destination NAT rule for the web-sv-02a web server virtual machine.

For upcoming labs, the internal IP address of both web server virtual machines must be translated.

1. Perform task 3 to add another IP address (172.20.11.6) to the uplink interface of perimeter gateway.

   NOTE

   You must use a comma to specify the second secondary IP address of the interface. Leave no space between the two IP addresses.

2. Perform task 4 to create a destination NAT rule on the perimeter gateway.

   Use the following parameters:

   - Assigned On: Uplink-Interface
   - Original Destination IP/Range: 172.20.11.6
   - Translated IP/Range: 10.1.10.12
   - Enabled: Select the check box.
   - Leave all other fields at the default value (undefined).

3. Above the NAT rules list, click **Publish Changes**.

4. Test your configuration.

   a. In the MTPuTTY window, begin capturing HTTP traffic on the uplink interface.

   ```
   debug packet display interface vNic_0 port_80
   ```

   b. In the browser, open a new browser tab and enter **`http://172.20.11.6`**.

   You should be able to reach the webpage.

   c. Close this browser tab.

   d. In the MTPuTTY window, verify that the correct two addresses are involved in the HTTP exchange.

   - 172.20.10.80
   - 172.20.11.6

   e. Press Ctrl+C to stop the packet capture.

   NOTE

   If the test does not produce the expected results, review your configuration carefully. Ensure that the destination NAT rule is enabled and that is applied on Uplink-Interface, and try the test again. If the test continues to fail, ask your instructor for help. Both destination NAT rules must be defined and working for upcoming labs.

Task 10: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. On the student desktop, leave the MTPuTTY window and the Command Prompt window open.
2. In the browser window, click the **vSphere Web Client** tab.
3. At the top of the Navigator pane, click the **Networking & Security** back arrow.
4. In the browser window, leave the **vSphere Web Client** tab open.
5. Leave the web-sv-01a console window open.

Lab 12 Configuring Load Balancing with NSX Edge Gateway

Objective: Configure a round-robin load balancer to distribute traffic between two web servers, and use traffic-capture tools to verify the round-robin operation

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Verify the Lack of Connectivity
3. Add an IP Address to the Uplink Interface of the Perimeter Gateway
4. Enable the Load Balancer Service and Configure an Application Profile
5. Create a Server Pool
6. Create a Virtual Server
7. Use the Packet Capture Capabilities of NSX Edge to Verify Round-Robin Load Balancing
8. Examine NAT Rule Changes
9. Migrate the Web-Tier Logical Switch to the Perimeter Gateway
10. Reposition the Virtual Server and Examine NAT Rule Changes
11. Use a Packet Capture to Verify Round-Robin Operation
12. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. On the student desktop, double-click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the MTPuTTY window is not open on the student desktop, open the MTPuTTY window.
   a. On the student desktop, double-click the **MTPuTTY** shortcut.
   b. In the MTPuTTY window, double-click the **Perimeter Gateway** saved session.
   c. If prompted to confirm a PuTTY security alert, click **Yes**.
   d. Log in as admin and enter the password **`VMware1!VMware1!`**.
3. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
4. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
5. When prompted, select the **Use Windows session authentication** check box and click **Login**.
6. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.
7. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.

Task 2: Verify the Lack of Connectivity

You open a web browser and browse to the IP address to be assigned to the load balancer virtual server.

1. Open a new browser tab and go to https://172.20.11.7.
2. Verify that the webpage does not open.

   The browser might display a `connection has timed out` message.
3. Close the new browser tab.
4. Click the **vSphere Web Client** tab.

Task 3: Add an IP Address to the Uplink Interface of the Perimeter Gateway

You configure an IP address for the uplink interface on the perimeter gateway so that it can receive incoming packets.

To use an IP address for network address translation (NAT) rules or a load balancer virtual server that is not the default IP address assigned to an NSX Edge interface, you must explicitly add the IP address to the interface. The IP address must be explicitly configured so that the NSX Edge appliance can receive incoming packets on that interface from the upstream device.

1. In the Navigator pane, select **NSX Edges**.
2. In the edge list, double-click the **Perimeter Gateway** entry to manage that object.
3. In the middle pane, click the **Manage** tab and click **Settings**.
4. In the settings category panel, select **Interfaces**.
5. In the interfaces list, select the **vNIC# 0** interface and click the pencil icon.

   The Edit NSX Edge Interface dialog box opens.
6. Under Configure Subnets, select the IP address entry and click the pencil icon.
7. Add **`172.20.11.7`** in the **Secondary IP address** text box.

   NOTE

   You must use a comma and leave no space between the IP addresses.
8. Click **OK** to commit the interface changes.

9. In the interfaces list, find the vNIC #0 entry, click the **Show All** link in the IP address column, and verify that the correct addresses appear in the list.

   - Primary address of the interface: 172.20.11.3
   - NAT address for web-sv-01a: 172.20.11.5
   - NAT address for web-sv-02a: 172.20.11.6
   - New address for the load balancer virtual server: 172.20.11.7

10. Click **OK** to close the Assigned IP Addresses dialog box.

Task 4: Enable the Load Balancer Service and Configure an Application Profile

You enable the load balancer service and configure for HTTPS with SSL pass-through.

1. Verify that **Perimeter Gateway** appears in the Navigator pane.
2. Click the **Manage** tab and click the **Load Balancer** tab.
3. In the Load Balancer category panel, select **Global Configuration**.
4. Click **Edit** on the right side of the global configuration page.
5. In the Edit load balancer global configuration page, select the **Enable Load balancer** check box, leave all the other fields at their default value, and click **OK**.
6. In the Load Balancer category panel, select **Application Profiles**.
7. Above the top panel, click the green plus sign to open the New Profile dialog box.
8. In the **Name** text box, enter **`App-Profile`**.
9. For Type, select **HTTPS**.
10. Select the **Enable SSL Passthrough** check box.
11. Leave all the other fields at their default value and click **OK**.

Task 5: Create a Server Pool

You create a round-robin server pool that contains the two web server virtual machines as members providing HTTPS.

1. In the Load Balancer category panel, select **Pools**.
2. Above the top panel, click the green plus sign to open the New Pool dialog box.
3. In the **Name** text box, enter **`Server-Pool`**.
4. Verify that the Algorithm selection is **ROUND-ROBIN**.
5. Verify that the Monitors selection is **NONE**.
6. Under Members, click the green plus sign to open the New Member dialog box, and add the first server.

Option	Action
Name	Enter **`Web-sv-01a`**.
IP Address	Enter **`10.1.10.11`**.
Port	Enter **`443`**.
All other settings	Leave at the default value.

7. Click **OK** to close the New Member dialog box.
8. Under Members, click the green plus sign to open the New Member dialog box, and add a second server.

Option	Action
Name	Enter **`Web-sv-02a`**.
IP Address	Enter **`10.1.10.12`**.
Port	Enter **`443`**.
All other settings	Leave at the default value.

9. Click **OK** to close the New Member dialog box.
10. Click **OK** to close the New Pool dialog box.

Task 6: Create a Virtual Server

The virtual server is positioned in a two-arm configuration on the external network that is attached to the uplink interface of the perimeter gateway.

1. In the Load Balancer category panel, select **Virtual Servers**.
2. Above the top panel, click the green plus sign to open the New Virtual Server dialog box.
3. Verify that the **Enable Virtual Server** check box is selected.
4. Verify that the Application Profile selection is **App-Profile**.
5. In the **Name** text box, enter **`VIP`**.
6. For the IP address, click the **Select IP Address** link, click **172.20.11.7**, and click **OK**.
7. From the **Protocol** drop-down menu, select **HTTPS**.
8. Verify that the port setting has changed to 443.
9. From the **Default Pool** drop-down menu, select **Server-Pool**.
10. Leave all other settings at their default value and click **OK**.

Task 7: Use the Packet Capture Capabilities of NSX Edge to Verify Round-Robin Load Balancing

You monitor the HTTPS traffic that traverses the transit network to verify round-robin distribution as the perimeter gateway assigns sessions to servers in the pool.

1. Minimize the browser window.
2. In the saved Perimeter Gateway MTPuTTY session window, begin capturing SSL packets on the transit interface.

   ```
   debug packet display interface vNic_1 port_443
   ```

3. Leave the packet capture running, and restore the browser window.
4. Open a new browser tab and go to https://172.20.11.7.
5. In the Your connection is not secure window, scroll down and click **Add Exception.**
6. Click **Confirm Security Exception** in the Add Security Exception pop-up window.
7. Click the browser refresh icon to display the website.
8. Minimize the browser window.

9. In the MTPuTTY window, examine the captured packets to determine source and destination addressing, and verify that the exchange is between a combination of the correct IP addresses.
    - 10.1.100.1
    - 10.1.10.11 or 10.1.10.12
10. Consider the packet exchange that you examined.

    Q1. Which extra operation is the perimeter gateway performing on packets that leave the transit network interface on the way to the web server virtual machines?

    Q2. Why is the perimeter gateway performing this extra operation instead of maintaining the original source address of the student desktop system?

    Q3. What setting would you enable on the load balancer so that the original source addresses are maintained?

11. Leave the packet capture running.
12. Restore the browser window, and click the **vSphere Web Client** tab.
13. In the Load Balancer category panel, select **Pools**.
14. In the pool list, select **pool-1** and click the pencil icon.

    The Edit Pool dialog box opens.
15. At the bottom, select the **Transparent** check box and click **OK**.
16. Open another tab in the browser window, and go to https://172.20.11.7.
17. Minimize the browser window.
18. In the MTPuTTY window, examine the captured packets to determine the source and destination addressing, and verify that the exchange is between a combination of the correct IP addresses.
    - 172.20.10.80.

      With transparent mode enabled, the original source address is maintained in packets forwarded to the web server. Sessions are still proxied by the perimeter gateway by using a source port different from the source port that is used by the original client.
    - 10.1.10.11 or 10.1.10.12

19. In the MTPuTTY window, examine the captured packets to determine the source and destination addressing, and verify that the exchange is between a combination of the correct IP addresses.

    - 172.20.10.80

    - 10.1.10.11 or 10.1.10.12.

      The address that appears in the most recent capture should be the web server that was not seen in the previous capture.

20. In MTPuTTY, press Ctrl+C to stop the packet capture.

21. Restore the browser window.

22. Click the **vSphere Web Client** tab.

Task 8: Examine NAT Rule Changes

You examine the autogenerated NAT rule that NSX created for the virtual server.

An NSX Edge instance automatically defines NAT rules for various features to facilitate the operation of those features.

1. On the **Manage** tab, click **NAT**.

2. In the NAT rules list, find the destination NAT rule that has VIP IP address in the Destination IP Address column, Load Balancer in the Description column, and a blank rule type.

   All other rules have a rule type of USER.

   The blank rule type is an autogenerated destination NAT rule that the system created as part of the virtual server configuration.

3. Examine the destination NAT rule.

4. Expand and examine the Original IP Address and Translated IP Address fields.

Q1. Is the original IP address being translated in any way by this rule?

Q2. Is the port range being translated in any way by this rule?

Q3. If this rule performs no apparent translation, why did the system define it?

Q4. Given that a virtual server uses a destination NAT rule to trigger member server selection, do you think that a virtual server can operate normally using a pool of member servers with IP addresses that are also defined by destination NAT rules?

Q5. Which interface is the destination NAT rule applied on?

Task 9: Migrate the Web-Tier Logical Switch to the Perimeter Gateway

You migrate the Web-Tier logical switch so that the network is connected directly to the perimeter gateway. The load balancer virtual server is moved to the directly connected Web-Tier network to show side-by-side operation of the load balancer.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the Navigator pane, select **NSX Edges**.
3. In the edge list, double-click the **Distributed Router** entry to manage that object.
4. In the middle pane, click the **Manage** tab and click **Settings**.
5. In the Settings category panel, select **Interfaces**,
6. In the interfaces list, select the **Web-Tier** entry and click the **disconnect** icon.
7. Wait for the update to complete, and verify that a disconnect icon appears in the Web-Tier Status column.
8. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.

9. In the Navigator pane, select **NSX Edges**.
10. In the edge list, double-click the **Perimeter Gateway** entry to manage that object.
11. In the middle pane, click the **Manage** tab and click **Settings**.
12. In the settings category panel, select **Interfaces**.
13. Select the **vNIC# 2** interface and click the pencil icon to open the Edit NSX Edge Interface dialog box.
14. In the **Name** text box, enter **`Web-Tier-Temp`**.
15. Verify that the Type selection is **Internal**.
16. Click the **Connected To > Select** link.
17. Click **Web-Tier** and click **OK**.
18. Under Configure Subnets, click the green plus sign.
19. In the **Primary IP address** text box, enter **`10.1.10.1`**.
20. The new interface that you are configuring on the perimeter gateway replaces the distributed router interface that you disconnected in step 5 by using the same IP address.
21. In the **Subnet Prefix Length** text box, enter **`24`**.
22. Click **OK** to commit the interface changes.

Task 10: Reposition the Virtual Server and Examine NAT Rule Changes

You reposition the virtual server to accommodate the one-armed architecture. And you examine the changes that occur in the NAT rules as result of the change.

1. Verify that **Perimeter Gateway** appears in the Navigator pane.
2. On the **Manage** tab, click **Load Balancer**.
3. In the Load Balancer category panel, select **Virtual Servers**.
4. In the virtual servers list, select the single virtual server that is defined and click the pencil icon.
5. In the Edit Virtual Server dialog box, change the IP Address field to **`10.1.10.1`** and click **OK**.

   For this example, the primary IP address of an interface is used for the virtual server.
6. On the **Manage** tab, click **NAT**.

7. In the NAT rules list, find the destination NAT rule that has 10.1.10.1 in the Original IP Address column.

   Q1. Has the system autoremoved the destination NAT rule for the old virtual server IP address of original VIP IP address?

   Q2. Is the new rule translating the original IP address or port in any way?

   Q3. Based on the virtual server destination NAT rules that you have examined so far, is there any difference in the actual operation performed by NSX Edge on traffic to be sent to a member server?

8. Examine each of the new destination NAT rule columns carefully, thinking back to the previous destination NAT rule that you examined when the virtual server was positioned on the Uplink-Interface network.

   Q4. Other than a primary interface IP address being used as the virtual server IP address in this example, what is the primary difference between the two positions in terms of traffic flow and sequence of operations on the edge device when traffic is received, transformed, and subsequently sent to a member server?

Task 11: Use a Packet Capture to Verify Round-Robin Operation

You use the same techniques learned so far to verify proxy mode operation.

1. Minimize the browser window.
2. In the saved perimeter gateway MTPuTTY session window, begin capturing SSL packets on the Web-Tier-Temp interface.

   ```
   debug packet display interface vNic_2 port_443
   ```

3. Leave the packet capture running, and restore the browser window.
4. Open a new browser tab and go to https://10.1.10.1.

   While you are performing the interim tasks in this lab, after migrating the Web-Tier virtual switch, the OSPF routing table automatically updates, and both the perimeter gateway and the distributed router are aware of the new network location.

5. When the browser reports a problem with the website’s certificate, click **Advanced.**
6. Scroll down and click **Add Exception**.
7. In the Add Security Exception pop-up window, click **Confirm Security Exception**.
8. Close the browser tab used to browse the webpage, and minimize the browser window.
9. In the MTPuTTY window, examine the captured packets and verify that the exchange is between a combination of the correct IP addresses.
   - 172.20.10.80

     At this point, the load balancer is still set to transparent mode. Thus the source that you should look for is the student desktop where the request originates.
   - 10.1.10.11 or 10.1.10.12

     The address that appears in the capture should be the web server not seen in the previous capture.
10. Press Ctrl+C to stop the packet capture.

Task 12: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. On the student desktop, leave the MTPuTTY window and the Command Prompt window open.
2. In the browser window, leave the **vSphere Web Client** tab open.
3. Close the browser tab for the 10.1.10.1 address.
4. Leave the web-sv-01a console window open.

Lab 13 Advanced Load Balancing

Objective: Configure a load balancer to provide SSL security for a website

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Generate a Certificate
3. Modify the Existing Load Balancer on the Perimeter Gateway
4. Capture Network Traffic at the Perimeter Gateway
5. Migrate the Web-Tier Logical Switch Back to the Distributed Router
6. Clean Up for the Next Lab

You must successfully complete lab 12 before you start this lab.

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. In the task bar of the student desktop, click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the MTPuTTY window is not open on the student desktop, open the MTPuTTY window.
   a. On the student desktop, double-click the **MTPuTTY** shortcut.
   b. In the MTPuTTY window, double-click the saved **Perimeter Gateway** session.
   c. If prompted to confirm a PuTTY security alert, click **Yes**.
   d. Log in as admin using the VMware1!VMware1! password.
3. If the Firefox window is closed, double-click the **Firefox** icon on the student desktop.
4. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
5. When prompted, select the **Use Windows session authentication** check box and click **Login**.
6. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.

Task 2: Generate a Certificate

You generate a certificate request and instruct the NSX Edge instance to create a self-signed certificate from that request.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the Navigator pane, select **NSX Edges**.
3. In the edge list, double-click the **Perimeter Gateway** entry to manage that object.
4. Click the **Manage** tab and click **Settings**.
5. In the Settings category panel, select **Certificates**.
6. Next to the gear sign, click **Actions**.
7. From the **Actions** drop-down menu, select **Generate CSR** to open the Generate CSR dialog box.
8. In the **Common Name** text box, enter **`10.1.10.1`**.
9. In the **Organization Name** text box, enter **`ABC Medical`**.
10. In **Organization Unit** text box, enter **`Audiology`**.
11. In the **Locality** text box, enter **`Palo Alto`**.
12. In the **State** text box, enter **`CA`**.
13. In the **Country** field, select **United States (US)**.
14. Verify that **RSA** is selected from the **Message Algorithm** drop-down menu.
15. Verify that **2048** is selected from the **Key Size** drop-down menu.
16. Leave all other settings at their default value and click **OK**.
17. In the certificate list, select the newly generated signing request.
18. Next to the gear sign, click **Actions**.
19. From the **Actions** drop-down menu, select **Self Sign Certificate**.
20. When prompted, enter **`365`** in the **Number of days** text box and click **OK**.

Task 3: Modify the Existing Load Balancer on the Perimeter Gateway

You update the application profile to include the self-signed certificate, and you update the server pool to use HTTP instead of HTTPS.

For this lab, you consider the web server as not having its own certificate. The self-signed certificate is used instead for communication between clients and the virtual server. Communication between the virtual server and the member servers uses HTTP.

1. On the **Manage** tab of Perimeter Gateway, click **Load Balancer**.
2. In the Load Balancer category panel, select **Application Profiles**.
3. Select the single application profile that is listed and click the pencil icon.
4. In the Edit Profile dialog box, select the service certificate.
   a. Deselect the **Enable SSL Passthrough** check box.
   b. At the bottom of the dialog box, click **Configure Service Certificate** and leave 10.1.10.1 selected in the certificate list.
   c. Leave all other settings at their default value and click **OK**.
5. In the load balancer category panel, select **Pools**.
6. Select the single pool that appears and click the pencil icon.
7. In the Edit Pool dialog box, update each member server that is listed.
   a. Select each member server and click the pencil icon.
   b. In the Edit Member dialog box, enter **`80`** in the **Port** and the **Monitor Port** text boxes and click **OK**.

   You must ensure that both member servers are updated.

Task 4: Capture Network Traffic at the Perimeter Gateway

You examine a packet capture on the uplink interface to verify the SSL communication between clients and the virtual server. You examine a packet capture on the transit network to verify round-robin operation.

1. Minimize the browser window.
2. In the saved Perimeter Gateway MTPuTTY session window, begin capturing SSL traffic on the uplink interface.

   ```
   debug packet display interface vNic_0 port_443
   ```

3. Leave the packet capture running, and position the window so that you remember that it contains the uplink capture.
4. In the MTPuTTY application, double-click **Perimeter Gateway** to open another PuTTY session.
5. Log in as admin and enter the **`VMware1!VMware1!`** password.
6. In the new PuTTY window, begin capturing HTTP traffic on the web-tier-temp interface.

   ```
   debug packet display interface vNic_2 port_80
   ```

   The two packet captures show the load balancer virtual server receiving SSL traffic and connecting to a pool member server using HTTP.

7. On the student desktop, open a new tab in the browser.
8. In the browser window, go to https://10.1.10.1.
9. Minimize the browser window.
10. Select the MTPuTTY window that contains the uplink interface (vNic_0) capture.
11. In the MTPuTTY window, examine the captured packets, and verify that the exchange is between a combination of the correct IP addresses.
    - 172.20.10.80
    - 10.1.10.1

      This address is the virtual IP address of the load balancer in the one-arm configuration.
12. Press Ctrl+C to stop the traffic capture.
13. Select the MTPuTTY window that contains the transit network (vNic_2) capture.

14. In the PuTTY window, examine the captured packets, and verify that the exchange is between a combination of the correct IP addresses.

    - 172.20.10.80

      This address is the IP address of the student system that is maintained in transparent mode.

    - 10.1.10.11 or 10.1.10.12

      This address is the IP address of one of the web servers on the Web-Tier logical switch.

15. Restore the browser window.
16. Close the browser tab.
17. Keep the original MTPuTTY window open.

Task 5: Migrate the Web-Tier Logical Switch Back to the Distributed Router

You restore the lab environment to its original state by migrating the Web-Tier logical switch back to the distributed router.

Subsequent labs will fail if the configuration is not restored.

1. Verify that **Perimeter Gateway** appears in the Navigator pane.
2. Click the **Manage** tab and click the **Load Balancer** tab.
3. In the Load Balancer category panel, select **Virtual Servers**.
4. Select the single virtual server that is listed and click the pencil icon to open the Edit Virtual Server dialog box.
5. Change the IP address field to 172.20.11.7.

   The virtual server IP address must be moved back to the uplink network because the Web-Tier logical switch is migrated back to the distributed router.

6. Click **OK**.
7. On the **Manage** tab, click **Settings**.
8. In the settings category panel, select **Interfaces**.
9. In the interface list, select the **Web-Tier-Temp** interface and click the disconnect icon.
10. Click **Yes** in the Disable Configuration pop-up window.
11. When the update completes, verify that a disconnect icon appears in the Web-Tier-Temp Status column.
12. Select the Web-Tier-Temp interface, click the red X to delete the interface.

13. When prompted to confirm the deletion, click **Yes**.

    You must delete the correct interface.

14. Wait for the update to complete, and verify that vNIC# 2 is reset.
15. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
16. In the Navigator pane, select **NSX Edges**.
17. In the edge list, double-click the **Distributed Router** entry to manage that object.
18. In the settings category panel, select **Interfaces**.
19. In the interface list, select the **Web-Tier** interface entry, and click the green check mark icon to reattach the logical switch.
20. Wait for the update to complete, and verify that a green check mark icon appears in the Web-Interface Status column.

Task 6: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. On the student desktop, leave the MTPuTTY window and the Command Prompt window open.
2. In vSphere Web Client, point to the **Home** icon and select **Networking & Security**.
3. In the browser window, leave the vSphere Web Client tab open.
4. Leave the web-sv-01a console window open.

Lab 14 Configuring Layer 2 VPN Tunnels

Objective: Configure an L2 VPN tunnel between two NSX Edge services gateway appliances

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Create a Port Group on the Distributed Switch for the Sink Port
3. Create a Trunk Interface for the Perimeter Gateway
4. Configure the Perimeter Gateway as an L2 VPN Server
5. Prepare the Remote Site for Setting Up an L2 VPN Tunnel
6. Create an NSX Edge Gateway at the Remote Site
7. Attach a Remote Web Tier Network to the Remote Gateway
8. Configure the Remote Gateway as an L2 VPN Client
9. Update the web-sv-01b Web Server Located at the Remote Site
10. Test Tunnel Connectivity
11. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. In the task bar of the student desktop, click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the MTPuTTY window is not open on the student desktop, open the MTPuTTY window.
   a. In the task bar of the student desktop, click the **MTPuTTY** shortcut.
   b. In the MTPuTTY window, double-click the saved **Perimeter Gateway** session.
   c. If prompted to confirm a MTPuTTY security alert, click **Yes**.
   d. Log in as admin and enter the password **`VMware1!VMware1!`**.
3. If the Firefox window is closed, double-click the **Firefox** icon in the task bar of the student desktop.
4. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
5. When prompted, select the **Use Windows session authentication** check box and click **Login**.
6. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.

Task 2: Create a Port Group on the Distributed Switch for the Sink Port

You create a port group on the distributed switch for the sink interface used by the L2 VPN feature.

1. Point to the vSphere Web Client **Home** icon and select **Networking**.
2. Expand the inventory tree and select **dvs-SA-Datacenter**.
3. In the middle pane, click **Actions** and select **Distributed Virtual Port Group > New Distributed Port Group**.
4. Enter `L2VPN-Trunk` in the **Name** text box in the New Distributed Port Group window.
5. Click **Next**.
6. On the Configure Settings page, leave the default settings and click **Next**.
7. Click **Finish** on the Ready to complete page.

Task 3: Create a Trunk Interface for the Perimeter Gateway

You create a trunk interface on the perimeter gateway for the L2 VPN feature. You remove the Web-Tier logical switch from the distributed logical router so that you can connect the Web-Tier logical switch as a subinterface on the perimeter gateway.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. Select **NSX Edges** in the Navigator pane.
3. Double-click **Distributed Router**.
4. Click the **Manage** tab and click **Settings**.
5. In the Settings category panel, select **Interfaces**.
6. Select the **Web-Tier** interface, and click the red X at the top to delete the configuration.
7. Click **OK** to confirm.
8. Click the back arrow next to **Networking & Security** in the Navigator pane.
9. Double-click **Perimeter Gateway** in the middle pane.
10. Click the **Manage** tab and click **Settings**.
11. In the Settings category panel, select **Interfaces**.
12. In the Interfaces list, select the **vnic2** row and click the pencil icon at the top.

    The Edit NSX Edge Interface window appears.
13. In the **Name** text box, enter `L2VPN-Trunk`.
14. From the **Type** drop-down menu, select **Trunk**.

15. For Connected To, click the **Select** link.

    The Connect NSX Edge to a Network window appears.

16. Click the **Distributed Virtual Portgroup** tab, select **L2VPN-Trunk**, and click **OK**.

17. Under Sub Interfaces, click the plus sign.

    The Add Sub Interface window appears.

18. In the **Name** text box, enter **`Subint-to-Web-Tier`**.

19. In the **Tunnel Id** text box, enter **`10`**.

20. For Backing Type, leave **Network** selected.

21. For Network, click the **Select** link and select the **Web-Tier** logical switch.

22. Click **OK**.

23. Under Configure Subnets, click the green plus sign.

24. Enter **`10.1.10.1`** in the **Primary IP address** text box.

    10.1.10.1 is the IP address of Subint-to-Web-Tier for the L2 VPN client edge gateway.

25. Enter **`24`** in the **Subnet Prefix Length** text box.

26. Click **OK**.

27. Click **OK**.

Task 4: Configure the Perimeter Gateway as an L2 VPN Server

You configure the L2 VPN server service on the perimeter gateway.

1. Verify that **Perimeter-Gateway** is selected in the Navigator pane.

2. Click the **Manage** tab and click **VPN**.

3. In the VPN category panel, select **L2VPN**.

4. For L2 VPN service status, click **Start**.

    IMPORTANT

    Do not click **Publish**.

5. For L2 VPN mode, ensure that **Server** is selected.

6. For Global Configuration Details, click **Change**.

7. Leave **Listener IP** as 172.20.11.3, which is your perimeter gateway's primary IP.

8. Leave **Listener Port** as 443.

9. For Encryption Algorithm, select **AES128-GCM-SHA256.**
10. Under Certificate Details, leave **Use System Generated Certificate** selected.
11. Click **OK**.
12. Under Site Configuration Details, click the green plus sign.
13. Select the **Enable Peer Site** check box.
14. In the **Name** text box, enter **`L2VPN`**.
15. In the **User ID** text box, enter **`vpnuser`**.
16. Enter **`VMware1!VMware1!`** in the **Password** and the **Confirm Password** text boxes.
17. For Stretched Interfaces, click **Select Sub Interfaces**.
18. In the Available Objects pane, select **Subint-to-Web-Tier** and click the blue right arrow.
19. Click **OK**.
20. In the Add Peer Site window, click **OK**.
21. Click **Publish Changes** at the top.
22. Verify that the L2 VPN service status is **Enabled**.

Task 5: Prepare the Remote Site for Setting Up an L2 VPN Tunnel

You create a port group on the distributed switch at the remote site for setting up L2 VPN connectivity.

1. In vSphere Web Client, point to the **Home** icon and select **Networking**.
2. Expand the SB-Datacenter and select **dvs-SB--Datacenter**.
3. Click **Actions** in the middle pane, and select **Distributed Port Group > New Distributed Port Group**.

   The New Distributed Port Group window appears.
4. In the **Name** text box, enter **`L2VPN-RemoteSite-Trunk`** and click **Next**.
5. On the Configure Settings page, leave the default setting and click **Next**.
6. Click **Finish**.
7. Repeat steps 3 through 6 to create an additional distributed port group named VPN-Web-Tier.

Task 6: Create an NSX Edge Gateway at the Remote Site

You add an NSX Edge gateway at the remote site for setting up L2 VPN connectivity between local and remote sites.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. Select **NSX Edges** in the Navigator pane, and select remote NSX Manager **172.20.110.43** from the **NSX Manager** drop-down menu.
3. Click the green plus sign in the middle pane to create an NSX Edge instance.
4. In the **Name** text box, enter **`Remote-Gateway`**, and leave all the other default settings.
5. Click **Next**.
6. Leave **User Name** as admin and enter **`VMware1!VMware1!`** in the **Password** and the **Confirm Password** text boxes.
7. Select the **Enable SSH Access** check box.
8. Click **Next**.
9. Click the green plus sign in the NSX Edge Appliance section.
10. From the **Cluster/Resource Pool** drop-down menu, select **SB-Management**.
11. Select **SB-Shared-01-Remote** for Datastore.
12. Leave all other options at their default and click **OK**.
13. On the Configure deployment page, click **Next**.
14. On the Configure interfaces page, click the green plus sign.

    The Add NSX Edge Interface window appears.
15. In the **Name** text box, enter **`Uplink-Interface`**.
16. For Type, leave **Uplink** selected.
17. For Connected To, click the **Select** link.

    The Connect NSX Edge to a Network window appears.
18. Click the **Distributed Virtual Portgroup** tab and select **pg-SB-Production**.
19. Click **OK**.
20. Click the green plus sign to configure subnets.
21. In the **Primary IP Address** text box, enter **`172.20.111.8`**.

    172.20.111.8 is the L2 VPN client edge Uplink-Interface IP address.
22. In the **Subnet prefix length** text box, enter **`24`**.

23. Click **OK** to close the Add NSX Edge Interface window.
24. On the Configure interfaces page, click **Next**.
25. In the **Gateway IP** text box on the Default gateway settings page, enter **`172.20.111.10`**.

    172.20.111.10 is the L2 VPN client edge gateway IP address.
26. Leave all other settings at their default and click **Next**.
27. On the Firewall and HA page, select the **Configure Firewall default policy** check box.
28. For Default Traffic Policy, click **Accept**.
29. Leave all settings at their default and click **Next**.
30. Click **Finish** on the Ready to complete page.
31. Monitor the progress until the NSX Edge deployment is complete.

Task 7: Attach a Remote Web Tier Network to the Remote Gateway

You create a logical switch and attach it to the new remote gateway.

1. Select **NSX Edges** in the Navigator pane.
2. Verify that **172.20.110.43** is selected from the **NSX Manager** drop-down menu.
3. Double-click **Remote-Gateway** in the middle pane.
4. Click the **Manage** tab and click **Settings**.
5. In the Settings category panel, click the **Interfaces** link.
6. Select **vnic1** in the list of interfaces and click the pencil icon at the top.

   The Edit NSX Edge interface window appears.
7. In the **Name** text box, enter **`L2VPN-Trunk-Client`**.
8. For Type, select **Trunk**.
9. For Connected To, click the **Select** link.

   The Connect NSX Edge to a Network window appears.
10. Click the **Distributed Virtual Portgroup** tab.
11. Select **L2VPN-RemoteSite-Trunk** and click **OK**.
12. Under Sub Interfaces, click the green plus sign.

    The Add Sub Interface window appears.
13. In the **Name** text box, enter **`Subint-to-Web-Tier`**.

14. Enter `10` in the **Tunnel Id** text box.

15. For Backing Type, leave **Network** selected.

    The Connect NSX Edge to a Network window appears.

16. For Network, click the **Select** link, click **Distributed Virtual Portgroup**, select **VPN-Web-Tier**, and click **OK**.

17. Under Configure Subnets, click the green plus sign.

18. In the **Primary IP Address** text box, enter `10.1.10.1`.

    10.1.10.1 is the IP address of Subint-to-Web-Tier for the L2 VPN client edge gateway.

19. In the **Subnet Prefix Length** text box, enter `24`.

20. Click **OK** to close the Add Sub Interface window.

21. Click **OK** to close the Edit NSX Edge Interface window.

Task 8: Configure the Remote Gateway as an L2 VPN Client

You configure the perimeter gateway as a VPN client.

1. Confirm that remote gateway is selected in the Navigator pane.

2. Click **Manage** and click **VPN**.

3. In the VPN category list, select **L2VPN**.

4. For L2VPN Mode on the L2VPN configuration page, click **Client**.

5. For Global Configuration Details, click **Change**.

   The Client Settings window appears.

   a. In the **Server Address** text box, enter `172.20.11.3`.

      172.20.11.3 is the L2 VPN server listener IP address.

   b. Verify that the listener port is 443.

   c. From the Encryption Algorithm list, select **AES128-GCM-SHA256**.

   d. For Stretched Interfaces, click the **Select Sub Interfaces** link.

e. In the Available Objects pane, select the **Subint-to-Web-Tier** object and click the blue right arrow.

f. Click **OK**.

g. In the User Details section, enter **`vpnuser`** in the **User Id** text box.

h. In the **Password** text box, enter **`VMware1!VMware1!`**.

i. In the **Re-Type Password** text box, enter **`VMware1!VMware1!`**.

j. Click **OK**.

6. For L2VPN Service Status, click **Start**.

7. Click **Publish Changes**.

8. Wait for the update to complete, and verify that the L2 VPN service status appears as Started.

9. At the bottom of the L2VPN configuration page, click **Refresh Status** and expand the **Tunnel Status** section.

10. Verify that the tunnel Status is Up.

    a. Expand the view of Tunnel Status.

    b. If the tunnel status is Down, wait a minute and click **Fetch Status**.

    c. If the tunnel remains down, review the lab thus far and verify that you made all configuration changes correctly.

Task 9: Update the web-sv-01b Web Server Located at the Remote Site

You change the networking configuration on the web-sv-01b web server located in the remote site inventory.

1. In vSphere Web Client, point to the **Home** icon and select **VMs and Templates**.

2. Select **web-sv-01b** in the left inventory pane.

3. In the middle pane, select **Power > Power On** from the **Actions** drop-down menu.

4. Open the console window of the web-sv-01b virtual machine.

    a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.

    b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01b**.

       This virtual machine is located at the Site-B data center.

    c. Click the **Summary** tab.

    d. Click the console thumbnail image.

    e. Enter the user name **`root`** and the password **`VMware1!`**.

5. At the web-sv-01b command prompt, change the IP address of the web-sv-01b virtual machine.

   ```
   ifconfig eth0 10.1.10.13 netmask 255.255.255.0
   ```

6. Change the default gateway used by the virtual machine.

   ```
   route add default gw 10.1.10.1 eth0
   ```

7. Verify that the IP address is assigned.

   ```
   ifconfig
   ```

8. Switch back to the **vSphere Web Client** tab in the browser.

Task 10: Test Tunnel Connectivity

You perform connectivity tests to determine the functional state of the L2 VPN tunnel.

1. In the inventory pane, select **Discovered virtual machine** > **web-sv-01b**.
2. Click **Actions** in the middle pane, and click the **Edit Settings** link.
3. From the **Network Adapter 1** drop-down menu, select the **VPN-Web-Tier** port group.
4. Click **OK** and click **OK**.
5. Restore the web-sv-01b console window from the Windows task bar.
6. At the web-sv-01b command prompt, view the network interface configuration.

   ```
   ifconfig
   ```

7. Record the eth0 hardware (HWaddr) address. __________
8. At the command prompt, ping the web-sv-01a VM on the Web-Tier logical switch of your vCenter Server system.

   ```
   ping 10.1.10.11
   ```

   Internet Control Message Protocol (ICMP) echo replies are received.

   a. Leave the `ping` command running.

   b. If ICMP echo replies are not received, press Ctrl+C to stop the `ping` command, wait for one minute, and repeat step 8.

9. Press Ctrl+Alt to release the pointer.

10. Consider the configuration.

    An L2 tunnel connects two NSX Edge gateways and extends the Web-Tier logical switch network. You have initiated a continuous ping from the Web server on the branch gateway side of the tunnel to the web server on the perimeter gateway side of the tunnel.

    Q1. If you capture traffic on the web-sv-01 virtual machine, on the perimeter gateway side of the tunnel, what is the source IP address that the incoming ping packets would have?

    Q2. What is the source hardware (MAC) address that the frames would have?

11. Restore the web-sv-01a console window from the Windows task bar.

12. At the web-sv-01a command prompt, examine the Address Resolution Protocol (ARP) table.

    ```
    arp -a
    ```

13. In the ARP table output, find the hardware address and the IP address of the web-sv-01b virtual machine.

    Q3. Is the hardware address the same that you recorded in step 7?

    Q4. Is this result what you expected?

    The hardware address for web-sv-01b is preserved when the tunnel traffic is decapsulated by the perimeter gateway. Because this is an L2 tunnel, response frames sent to that MAC address are intercepted for encapsulation back to the sending node. This tunnel differs from an IPsec tunnel, for example, where you might see the source IP with the hardware address of the gateway interface that faces the destination.

Task 11: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Leave the MTPuTTY window open.
2. Leave the Command Prompt window open.
3. Restore the browser window.
4. In the web-sv-01b console tab, press Ctrl+C to stop the `ping` command.
5. In the browser window, leave the **vSphere Web Client** tab open.
6. Leave the web-sv-01a and web-sv-01bconsole windows open.

Lab 15 Configuring IPsec Tunnels

Objective: Configure, test, and troubleshoot an IPsec tunnel designed to connect the headquarters site and the branch site

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Prepare the Perimeter Gateway for IPsec Tunneling
3. Configure the Perimeter Gateway as an IPsec Tunnel Endpoint
4. Prepare the Remote Gateway for IPsec Tunneling
5. Update the web-sv-01b Web Server in the vCenter Server Inventory of the Remote Site
6. Configure the Remote Gateway as an IPsec Tunnel Endpoint
7. Test VPN Tunnel Connectivity
8. Disable IPsec on the Perimeter Gateway and Enable OSPF
9. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. On the student desktop, double-click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.

2. If the MTPuTTY window is not open on the student desktop, open the MTPuTTY window.
   a. On the student desktop, double-click the **MTPuTTY** shortcut.
   b. In the MTPuTTY window, double-click the saved **Perimeter Gateway** session.
   c. If prompted to confirm a PuTTY security alert, click **Yes**.
   d. Log in as admin and enter the password **`VMware1!VMware1!`**.
3. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
4. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
5. When prompted, select the **Use Windows session authentication** check box and click **Login**.
6. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the Site-A-Datacenter inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.
7. If the web-sv-01b console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the SB-Datacenter inventory tree and select **Discovered virtual machine** > **web-sv-01b**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.

Task 2: Prepare the Perimeter Gateway for IPsec Tunneling

You perform the necessary configuration changes to enable IPsec tunneling on the perimeter gateway.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. Select **NSX Edges** in the Navigator pane, and verify that **172.20.10.42** is selected from the **NSX Manager** drop-down menu.
3. In the edge list, double-click the **Perimeter-Gateway** entry to manage that object.
4. In the middle pane, click the **Manage** tab and click **VPN**.
5. In the VPN category panel, select **L2VPN**.
6. In the L2VPN Service Configuration row, click **Delete Configuration**.
7. Click **Yes** to confirm the deletion.
8. Wait for the update to complete, and verify that the L2VPN configuration is reset and that L2VPN Service Status is Disabled.

   The update might take a few minutes to complete.
9. Under Manage, click **Routing**.
10. In the Routing category panel, select **OSPF**.
11. In the OSPF Configuration panel, click **Edit**.
12. In the OSPF Configuration dialog box, deselect the **Enable OSPF** check box and click **OK**.

    The perimeter gateway is configured as an IPsec tunnel endpoint exposing the Web-Tier network. The networks that are exposed by an IPsec tunnel endpoint must be either direct-attached subnets or subnets reachable through static routing. You cannot expose subnets that are reachable only through a dynamic routing update from OSPF or one of the other supported routing protocols.
13. Click **Publish Changes** and wait for the update to complete.

    The update might take a few minutes to complete.
14. In the routing category panel, select **Static Routes**.

15. Click the green plus sign to open the Add Static Route dialog box.

    a. In the **Network** text box, enter **`10.1.0.0/16`**.

       10.1.0.0/16 is the workload VM network.

    b. In the **Next Hop** text box, enter **`10.1.100.2`**.

       This address is the interface address of the distributed router uplink interface on the transit network.

    c. From the **Interface** drop-down menu, select **Transit-Network**.

    d. Click **OK**.

16. Click **Publish Changes** and wait for the update to complete.

Task 3: Configure the Perimeter Gateway as an IPsec Tunnel Endpoint

You configure the perimeter gateway as an IPsec VPN tunnel endpoint that provides tunnel-based access to the Web-Tier network.

1. Verify that **Perimeter Gateway** appears in the Navigator pane.

2. Click **Manage** and click **VPN**.

3. In the VPN category panel, select **IPsec VPN**.

4. Above the tunnel endpoint list, click the green plus symbol icon to open the Add IPsec VPN dialog box.

5. Verify that the **Enabled** check box is selected.

6. In the **Name** text box, enter **`Local-Remote`**.

7. In the **Local Id** text box, enter **`Local`**.

8. In the **Local Endpoint** text box, enter **`172.20.11.3`**.

   172.20.11.3 is the IP address of the perimeter gateway. This address is the same address that identified the perimeter gateway as an L2 VPN server in lab 14.

9. In the **Local Subnets** text box, enter **`10.1.10.0/24`**.

   Spaces are not allowed in the local subnets specification. You must enter the specification exactly as shown.

10. In the **Peer Id** text box, enter **`Remote`**.

11. In the **Peer Endpoint** text box, enter **`172.20.111.8`**.

12. 172.20.118.8 is the IP address of the remote gateway.

13. In the **Peer Subnets** text box, enter **`10.2.40.0/24`**.

14. For Encryption Algorithm, leave **AES** selected.

15. Leave **PSK** selected.
16. In the **Pre-Shared key** text box, enter `VMware1!`.
17. Select the **Display shared key** check box, and verify that the shared key is exactly VMware1!.
18. Leave all remaining settings at the default value and click **OK**.
19. In the top status panel, click **Start** for IPsec VPN Service Status.
20. Click **Publish Changes** and wait for the update to complete.
21. In the status panel, verify that the IPsec VPN service status is Started.

Task 4: Prepare the Remote Gateway for IPsec Tunneling

You configure the remote gateway to enable IPsec VPN tunneling.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. Select **NSX Edges** in the Navigator pane, and select **172.20.110.43** from the **NSX Manager** drop-down menu.
3. In the edge list, double-click the **Remote-Gateway** entry to manage that object.
4. In the middle pane, click the **Manage** tab and click **VPN**.
5. In the VPN category panel, select **L2VPN**.
6. In the L2VPN Service Configuration row, click **Delete Configuration**.
7. Click **Yes** when prompted to confirm.
8. Wait for the update to complete, and verify that the **L2VPN** configuration is reset and that the service status is Disabled.

   The update might take up to a minute to complete.
9. On the **Manage** tab, click **Settings**.
10. In the settings category panel, select **Interfaces**.
11. In the interface list, select the **L2VPNTrunk-Client** interface and click the pencil icon.

    The Edit NSX Edge Interface window appears.
12. Under Sub Interface, select **Subint-to-Web-Tier** and click the pencil icon.

    The Edit Sub Interface window appears.

13. Under Configure Subnets, select **10.1.10.1** and click the pencil icon.
14. Change the primary IP address to 10.2.40.1, which is the IP address of the remote gateway's Web-Tier subinterface.
15. Click **OK** to close the Edit Sub Interface dialog box.
16. Click **OK** to commit the interface changes.

Task 5: Update the web-sv-01b Web Server in the vCenter Server Inventory of the Remote Site

You change the networking configuration on web-sv-01b to match the branch topology.

1. Restore the console window for web-sv-01b from the Windows task bar.
2. At the web-sv-01b command prompt, change the IP address of the web-sv-01b virtual machine.

   ```
   ifconfig eth0 10.2.40.11 netmask 255.255.255.0
   ```
3. Change the default gateway used by the virtual machine.

   ```
   route add default gw 10.2.40.1 eth0
   ```
4. Verify that the IP address is assigned correctly.

   ```
   ifconfig
   ```
5. Verify that the default gateway is configured correctly.

   ```
   route
   ```

Task 6: Configure the Remote Gateway as an IPsec Tunnel Endpoint

You configure a remote gateway as an IPsec VPN tunnel endpoint that provides tunnel-based access to the remote Web-Tier network.

1. In the web-sv-01b console window, press Ctrl+Alt to release the pointer.
2. Restore the **vSphere Web Client** tab in the browser.
3. Verify that **Remote Gateway** appears in the Navigator pane.
4. In the middle pane, click the **Manage** and click **VPN**.
5. In the VPN category panel, select **IPsec VPN**.
6. Above the tunnel endpoint list, click the green plus sign to open the Add IPsec VPN dialog box.
7. Verify that the **Enabled** check box is selected.
8. In the **Name** text box, enter **`Local-Remote`**.
9. In the **Local Id** text box, enter **`Remote`**.

10. In the **Local Endpoint** text box, enter **`172.20.111.8`**.

    172.20.111.8 is the IP address of the remote gateway.

11. In the **Local Subnets** text box, enter **`10.2.40.0/24`**.

    10.2.40.0/24 is the remote subnet.

12. In the **Peer Id** text box, enter **`Local`**.

13. In the **Peer Endpoint** text box, enter **`172.20.11.3`**.

    172.20.11.3 is the IP address of the perimeter gateway.

14. In the **Peer Subnets** text box, enter **`10.1.10.0/24`**.

    10.1.10.0/24 is the local subnet.

15. Leave **AES** selected as the Encryption Algorithm.

16. Leave **PSK** selected.

    a. In the **Pre-Shared key** text box, enter **`VMware1!`**.

    b. Select the **Display shared key** check box, and verify that the shared key is exactly VMware1!.

    c. Leave all remaining settings at their default value and click **OK**.

17. For IPsec VPN Service Status, click **Start**.

18. Click **Publish Changes** and wait for the update to complete.

19. In the status panel, verify that the IPsec VPN service status is Enabled.

Task 7: Test VPN Tunnel Connectivity

You use `ping` tests to determine the connectivity status of the IPsec VPN tunnel.

1. When the VPN tunnels is established, click the **Show IPsec Statistics** link.
2. In the IPsec VPN Statistics pop-up window, verify the VPN connection configuration.
   - Name: Local-Remote
   - Local Endpoint: 172.20.111.8
   - Peer Endpoint: 172.20.11.3
   - Channel Status: Green check mark
   - Tunnel Status: 1 UP 0 DOWN
3. Select the single connection listed in the top table.
4. Verify that a single tunnel is listed in the bottom table.
   - Local Subnets: 10.2.40.0/24
   - Peer Subnets: 10.1.10.0/24
   - Tunnel State: Green check mark
5. Close the IPsec VPN Statistics pop-up window.
6. Verify that the established VPN connection between the two NSX Edge gateway appliances is listed in the table and the tunnel is open.
   - Name: Local-Remote
   - Local Endpoint: 172.20.111.8
   - Local Subnets: 10.2.40.0/24
   - Peer Endpoint: 172.20.11.3
   - Peer Subnets: 10.1.10.0/24
   - Status: Green check mark
7. Restore the web-sv-01b console window from the Windows task bar.
8. At the web-sv-01b command prompt, start a ping to the web-sv-01a virtual machine at 10.1.10.11.

   ```
   ping 10.1.10.11
   ```

   The ping should be successful, confirming connectivity between the two sites using IPsec VPN.
9. Press Ctrl+C to stop the ping.

Task 8: Disable IPsec on the Perimeter Gateway and Enable OSPF

You disable IPsec on the perimeter gateway. You enable OSPF on the perimeter gateway to establish routing.

1. Restore the **vSphere Web Client** tab in the browser.
2. Point to the **Home** icon of the vSphere Web Client and select **Networking & Security**.
3. Select **NSX Edges** in the Navigator pane, and ensure that **172.20.10.42** is selected from the **NSX Manager** drop-down menu.
4. Double-click **Perimeter Gateway** to open the configuration of your perimeter gateway.
5. Click **Manage** tab and click **VPN**.
6. In the VPN category panel, select **IPsec VPN**.
7. In the IPsec VPN Service Status row, click **Stop**.
8. Click **Publish Changes** and wait for the screen to update.
9. On the **Manage** tab, click the **Routing** tab.
10. In the Routing category panel, select **OSPF**.
11. In the OSPF Configuration row, click **Edit**.
12. In the OSPF Configuration pop-up window, select the **Enable OSPF** check box.
13. Click **OK**.
14. Click **Publish Changes**.

Task 9: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Leave the MTPuTTY window open.
2. Leave the Command Prompt window open.
3. Close the web-sv-01b console tab.
4. Click the **vSphere Web Client** tab for the remote site.
5. At the top of the Navigator pane, click the **Networking & Security** left arrow.
6. In the browser window, leave the **vSphere Web Client** tab open.
7. Leave the web-sv-01a console window open.

Lab 16 Configuring and Testing SSL VPN-Plus

Objective: Configure an SSL VPN-Plus portal page and a direct-access client package

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Configure SSL VPN-Plus Server Settings on the Remote Gateway
3. Configure a Local Authentication Server and a Local User on the Remote Gateway
4. Enable SSL VPN-Plus on the Remote Gateway, and Test Portal Access
5. Configure an IP Pool and Private Networks
6. Create and Test an Installation Package
7. Use the SSL VPN-Plus Client Application to Test Network Access
8. Review the Client Configuration, and Examine Traffic
9. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of the VMware vSphere® Web Client interface.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. In the task bar of the student desktop, click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the MTPuTTY window is not open on the student desktop, open the MTPuTTY window.
   a. In the task bar of the student desktop, click the **MTPuTTY** shortcut.
   b. In the MTPuTTY window, double-click the saved **Perimeter Gateway** session.
   c. If prompted to confirm a PuTTY security alert, click **Yes**.
   d. Log in as admin and enter the password **`VMware1!VMware1!`**.
3. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
4. When prompted, select the **Use Windows session authentication** check box and click **Login**.
5. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client Home icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.
6. Point to the vSphere Web Client **Home** icon and select **Inventories** > **Networking & Security**.

Task 2: Configure SSL VPN-Plus Server Settings on the Remote Gateway

You configure SSL VPN-Plus to enable the remote gateway at your remote site to act as a VPN server.

1. Select **NSX Edges** in the Navigator pane, and ensure that **172.20.110.43** is selected from the **NSX Manager** drop-down menu.
2. In the edge list, double-click the **Remote-Gateway** entry to manage that object.
3. In the middle pane, click the **Manage** tab and click **SSL VPN-Plus**.
4. In the SSL VPN-Plus category panel, select **Server Settings** and click **Change**.
5. In the Change Server Settings dialog box, configure the server settings.
   a. For IPv4 Address, leave the **172.20.111. 8 (Primary)** address selected.
   b. For IPv6 Address, leave **None** selected.
   c. Leave the port specification of **443**.
   d. For Cipher List, select **AES256-SHA**.
   e. For Server Certificate, leave the **Use Default Certificate** check box selected.
   f. Click **OK**.

Task 3: Configure a Local Authentication Server and a Local User on the Remote Gateway

You configure the remote gateway to provide local authentication services.

1. In the SSL VPN-Plus category panel, select **Authentication**.
2. In the middle pane, click the green plus sign icon to open the Add Authentication Server dialog box.
3. From the **Authentication Server Type** drop-down menu, select **LOCAL**.
4. Deselect the **Enable password policy** check box.
5. Deselect the **Enable account lockout policy** check box.
6. Leave all other settings at their default value and click **OK**.
7. In the SSL VPN-Plus category panel, select **Users**.
8. In the middle pane, click the green plus sign to open the Add User dialog box.
9. In the **User ID** text box, enter **`vpnuser`**.
10. In the **Password** text box and the **Re-type Password** text box, enter **`VMware1!`**.
11. Select the **Password never expires** check box.
12. Leave all other settings at their default value and click **OK**.

Task 4: Enable SSL VPN-Plus on the Remote Gateway, and Test Portal Access

You enable SSL VPN-Plus and test portal access through a browser.

1. In the SSL VPN-Plus category panel, select **Dashboard**.
2. In the Status panel, click **Start** for Service.
3. Click **Yes** when prompted to confirm.
4. Wait for the update to complete, and verify that the service status is Started.
5. Open a new browser tab and go to https://172.20.111.8.

   172.20.111.8 is the remote gateway IP address.
6. When prompted with the website's certificate warning, click **Advanced**.
7. Scroll down and click **Add Exception**.
8. Click **Confirm Security Exception** in the Add Security Exception pop-up window.
9. On the VMware SSL VPN-Plus portal page, log in as vpnuser, enter the password **`VMware1!`**, and click **Login**.
10. On the user portal page, verify that one tab labeled **Tools** appears with a **Change Password** link available.
11. Click **Logout**, and click **OK** when prompted to confirm.
12. Close the portal tab.

Task 5: Configure an IP Pool and Private Networks

You configure an IP pool and private networks in preparation for direct network connectivity by an SSL VPN-Plus client.

1. In the SSL VPN-Plus category panel, select **IP Pool.**
2. On the IP Pool configuration page, click the green plus sign to open the Add Static IP Pool dialog box.
3. In the first **IP Range** text box, enter **`192.168.170.2`**.
4. In the second **IP Range** text box, enter **`192.168.170.254`**.
5. In the **Netmask** text box, enter **`255.255.255.0`**.
6. In the **Gateway** text box, enter **`192.168.170.1`**.
7. Leave all other settings at the default value and click **OK**.
8. In the SSL VPN-Plus category panel, select **Private Networks**.

9. On the Private Networks configuration page, click the green plus sign to open the Add Private Networking dialog box.
10. Enter the remote site network **`10.2.40.0/24`** in the **Network** text box.
11. Leave all other settings at their default value and click **OK**.

Task 6: Create and Test an Installation Package

You create, configure, and test an installation package.

1. In the SSL VPN-Plus category panel, select **Installation Package**.
2. On the Installation Package configuration page, click the green plus sign to open the Add Installation Package dialog box.
   a. In the **Profile Name** text box, enter **`Test-Package`**.
   b. In the Gateway table, enter **`172.20.111.8`** in the Gateway column text box, leave the port as 443, and click **OK** in the same row to confirm the entry.
   c. In the Installation Parameters for Windows list, select the **Allow remember password**, **Enable silent mode installation**, and **Create desktop icon** check boxes.
   d. Click **OK**.
3. Open a new browser tab and go to https://172.20.111.8.
4. When prompted to log in, log in as vpnuser, enter the password **`VMware1!`**, and click **Login**.

   The SSL VPN-Plus portal appears.
5. On the **Full Access** tab, click the **Test Package** link.

   A new browser window appears.
6. In the new browser window, click **Please click here** to start the installation link.
7. When the `You have chosen to open: VMware_VPN_Client-Setup.zip` message appears, click **Open with Windows Explorer (default)**.
8. In the new Windows Explorer window, double-click the **Intstaller.exe** file.
9. When the Compressed (zipped) Folders pop-up window appears, click **Extract all**.
10. When the Extract Compressed (Zipped) Folders window appears, click **Extract**.
11. In the next Windows Explorer window, double-click **Intstaller.exe.**
12. When the `Open File - Security Warning - Do you want to run this file?` message appears, click **Run**.

    The SSL VPN-Plus test package is installed on the student desktop.

13. Close the new Windows Explorer windows that opened when you started the installation.
14. In the SSL VPN-Plus portal, click the **Logout** link in the black status bar in the upper-right corner of the page, and click **OK** when prompted to confirm.
15. Close the portal tab.

Task 7: Use the SSL VPN-Plus Client Application to Test Network Access

You use the SSL VPN-Plus client application to test direct access to networks available through the SSL VPN-Plus tunnel.

1. Minimize the browser window.
2. In the Command Prompt window of the student desktop, try to ping web-sv-01b located in the remote site vCenter Server inventory.

   ```
   ping 10.2.40.11
   ```

   The `ping` command does not receive Internet Control Message Protocol (ICMP) echo replies.
3. Leave the Command Prompt window open.
4. On the student desktop, find a new shortcut called **VMware Tray**.

   The **VMware Tray** shortcut was added when the SSL VPN-Plus test package was installed from the portal page.
5. Double-click the **VMware Tray** shortcut to start the SSL VPN-Plus client application.
6. From the **Network** drop-down menu, leave **Test Package** selected and click **Login**.
7. Click **Yes** in the pop-up Security Alert window.
8. Log in as vpnuser, enter the password **`VMware1!`**, and click **OK**.
9. When the `SSL VPN connection established with network Test Package` message appears, click **OK**.
10. In the Command Prompt window, ping web-sv-01b:

    ```
    ping 10.2.40.11
    ```

    The `ping` command receives ICMP echo replies.

Task 8: Review the Client Configuration, and Examine Traffic

You review the SSL VPN-Plus client configuration. You use traffic-capture tools to verify tunnel connectivity.

1. On the student desktop, double-click the **VMware Tray** shortcut.

   When the SSL VPN-Plus client is running, double-clicking the program icon opens the statistics window. The statistics window can also be opened from the client application icon that is running in the system tray.

2. In the SSL VPN-Plus Client - Statistics window, click the **Advanced** tab.

   Q1. What is the gateway address and port for the network configuration?

   Q2. Which local subnets are exposed to the tunnel client?

   Q3. Which IP address is assigned to the encapsulated packets that traverse the tunnel?

3. On the student desktop, double-click the **MTPuTTY** shortcut.
4. Select **Server > Add Server**.
5. In the **Server Name** text box, enter **`172.20.111.8`**, and select **SSH** as the protocol.

   172.20.111.8 is the IP address of the remote gateway.

6. In the **Display name** text box, enter **`Remote-Gateway`** and click **OK**.
7. In the MTPuTTY window, double-click **Remote-Gateway** in the left pane.
8. When prompted with a PuTTY security alert, click **Yes**.
9. Log in as admin and enter the password **`VMware1!VMware1!`**.
10. Begin capturing ICMP packets on the internal network.

    ```
    debug packet display interface vNic_1 icmp
    ```

    Q4. If you capture packets on the NSX Edge side of the SSL VPN-Plus tunnel, on an interface connected to the destination subnet, what source IP address do ping packets have?

11. Leave the packet capture running.

12. Switch to the Command Prompt window and ping web-sv-01b.

    ```
    ping 10.2.40.11
    ```

13. Switch to the MTPuTTY window and verify that an ICMP exchange occurred between the IP addresses.

    - An IP address in the range of 192.168.170.2-192.168.170.254

      This address is assigned to the SSL VPN-Plus client adapter on the student desktop.

    - 10.2.40.11

14. Press Ctrl+C to stop the packet capture.

15. Close the MTPuTTY window for the remote gateway.

16. Minimize MTPuTTY.

17. On the student desktop, double-click the **VMware Tray** icon.

18. On the **General** tab, click **Logout** and click **Yes** when prompted to confirm.

Task 9: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Leave the MTPuTTY window open.
2. Leave the Command Prompt window open.
3. Restore the browser window.
4. Click the **vSphere Web Client** tab in the browser window.
5. Verify that you are in the Networking & Security inventory view.
6. In the browser window, leave the **vSphere Web Client** tab open.
7. Leave the web-sv-01a console window open.

Lab 17 Using NSX Distributed Firewall Rules to Control Network Traffic

Objective: Define NSX distributed firewall rules to restrict traffic to web servers and between application tiers

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Create a Distributed Firewall Section
3. Configure Cross-Tier Rules
4. Restrict Inbound Web Server Traffic to HTTP and HTTPS
5. Review Distributed Firewall Log Entries
6. Restore a Saved Distributed Firewall Configuration
7. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. In the task bar of the student desktop, click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the MTPuTTY window is not open on the student desktop, open the MTPuTTY window.
   a. On the student desktop, double-click the **MTPuTTY** shortcut.
   b. In the MTPuTTY window, double-click the saved **Perimeter Gateway** session to connect to the perimeter gateway.
   c. If prompted to confirm a PuTTY security alert, click **Yes**.
   d. Log in as admin using the **`VMware1!VMware1!`** password.
3. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
4. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
5. When prompted, select the **Use Windows session authentication** check box and click **Login**.
6. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.

Task 2: Create a Distributed Firewall Section

You create a section that contains your custom firewall rules.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security.**
2. Select **Firewall** in the Navigator pane, and select **172.20.110.42** (Site-A NSX Manager) from the **NSX Manager** drop-down menu in the middle pane.
3. On the **Configuration** tab, verify that the **General** tab is clicked.
4. In the list, find the **Default Section Layer3** entry.
5. If necessary, use the horizontal scroll bar to uncover the icons that appear on the far right of the default section.
6. Click the **folder** icon.
7. In the New Section pop-up configuration panel, create a section.
   a. In the **Section name** text box, enter **`Test-Section`**.
   b. Leave **Add above** selected.
   c. Click **Save**.
8. Click **Publish Changes** and wait for the update to complete.

Task 3: Configure Cross-Tier Rules

You configure rules to allow basic connectivity between the Web-Tier, App-Tier, and DB-Tier networks.

1. Locate the Test Section entry and click the green plus sign to create a rule.

   If necessary, use the horizontal scroll bar to locate the icons on the far-right side.
2. Expand Test Section and find the new rule entry.
3. Point to the **Name** cell and click the pencil icon.
4. In the **Rule Name** text box, enter **`Allow-Web-to-App`** and click **Save**.
5. Point to the **Source** cell and click the pencil icon to open the Specify Source configuration panel.
6. From the **Object Type** drop-down menu, select **Logical Switch**.
7. In the Available Objects pane, select **Web-Tier** and click the blue right arrow to move the switch into the Selected Objects list.
8. Click **OK**.
9. Point to the **Destination** cell and click the pencil icon to open the Specify Destination configuration panel.
10. From the **Object Type** drop-down menu, select **Logical Switch**.

11. In the Available Objects pane, select **App-Tier** and click the blue right arrow to move the switch into the Selected Objects list.
12. Click **OK**.
13. Point to the **Services** cell and click the pencil icon to open the Specify Service configuration panel.
14. In the lower-left corner of the pop-up panel, click the **New Service** link.
15. Enter the details in the Add Service dialog box.

Option	Action
Name	Enter **`Tomcat-8443`**.
Description	Leave blank.
Protocol	Select **TCP** from the drop-down menu.
Destination ports	Enter **`8443`**.
Enable inheritance...	Leave at the default value (deselected).

16. Click **OK**.
17. Click **OK**.
18. Click **Publish Changes** and wait for the update to complete.
19. Click the green plus sign above the rules list to create a rule.

NOTE

If the green plus sign is not active, select any rule in the Test Section rule list.

20. Point to the **Name** cell and click the pencil icon.
21. In the **Rule Name** text box, enter **`Allow-App-to-DB`** and click **OK**.
22. Point to the **Source** cell and click the pencil icon to open the Specify Source configuration panel.
23. Select **Logical Switch** from the **Object Type** drop-down menu.
24. Select **App-Tier** from the Available Objects list and click the blue right arrow to move the switch into the Selected Objects list.
25. Click **OK**.
26. Point to the **Destination** cell and click the pencil icon to open the Specify Destination configuration panel.

27. From the **Object Type** drop-down menu, select **Logical Switch**.
28. From the Available Objects list, select **DB-Tier** and click the blue right arrow to move the switch into the Selected Objects list.
29. Click **OK**.
30. Point to the **Services** cell and click the pencil icon to open the pop-up configuration panel.
31. In the Filter text box, enter `SQL`.
32. In the Available services list, scroll down to the generic **MySQL** service.
33. Select the **MySQL** service, and click the blue right arrow to move the service to the Selected Objects list.
34. Click **OK**.
35. Click **Publish Changes** and wait for the update to complete.

Task 4: Restrict Inbound Web Server Traffic to HTTP and HTTPS

You configure a firewall rule that restricts network traffic that is destined for a web server to HTTP and HTTPS.

1. Open a new browser tab and go to https://10.1.10.11.

   10.1.10.11 is the IP address of the web-sv-01a Web server on the Web-Tier logical switch network.
2. Verify that the webpage is displayed or that you are prompted with an untrusted connection message, and close the browser tab.
3. Return to vSphere Web Client.
4. In the firewall section list, expand the **Default Section Layer3** entry.
5. Point to the **Action** cell of Default Rule and click the pencil icon.
6. From the **Action** drop-down menu, select **Block**.
7. Click **Log** and click **Save**.
8. Click **Publish Changes** and wait for the update to complete.
9. Open a new browser tab and go to https://10.1.10.11.
10. Verify that the webpage is not displayed and close the browser tab.
11. If the webpage is displayed, click the browser refresh icon to reload the page.

    If your browser cached the page, you might have to clear the cache for the test.
12. Return to vSphere Web Client.

13. Click the green plus sign inline with the Test-Section to create a rule in Test-Section.

    If the icon is not active, you can select any rule in the Test-Section rule list and click the green plus sign.

14. Point to the **Name** cell and click the pencil icon.

15. In the **Rule Name** text box, enter `Allow-to-Web-Servers` and click **Save**.

16. Point to the **Destination** cell and click the pencil icon to open the Specify Destination configuration panel.

17. From the **Object Type** drop-down menu, select **Logical Switch**.

18. From the Available Objects list, select **Web-Tier** and click the blue right arrow to move the **Web-Tier** entry to the Selected Objects list on the right.

19. Click **OK**.

20. Point to the **Services** cell and click the pencil icon to open the **Specify Service** configuration panel.

21. Enter **HTTP** in the **Filter** text box.

22. In the Available Objects list, select the generic **HTTP** and **HTTPS** services and click the blue right arrow to move them to the Selected Objects list.

23. Click **OK**.

24. Point to the **Action** cell and click the pencil icon that appears.

25. Verify that **Allow** is selected from the **Actions** menu and click **Save**.

26. Click **Publish Changes** and wait for the update to complete.

27. Open a new browser tab and go to https://10.1.10.11.

28. Verify that the webpage is displayed or that you are prompted with an untrusted connection message, and close the browser tab.

29. Return to vSphere Web Client.

30. Point to **Web-Tier** in the **Destination** cell and click the red X that appears in the cell, to remove Web-Tier from the **Destination** cell.

31. Point to the **Destination** cell and click the **IP** icon that appears in the cell.

32. In the pop-up configuration panel, add the IP address of the web server.

    a. Leave **IPv4** selected.

    b. Enter `10.1.10.11` in the **Value** text box.

    c. Click **Save**.

33. Click **Publish Changes** and wait for the update to complete.

34. Open a new browser tab and go to https://172.20.11.5.

    172.20.11.5 is the destination NAT address that you configured in lab 12 for the web-sv-01a web server.

35. Click the browser page refresh icon to reload the page.

36. Verify that the webpage is displayed or that you are prompted with an untrusted connection message, and close the browser tab.

37. Return to vSphere Web Client.

38. Read the summary.

    In the previous lab, attempts to browse the destination NAT address were blocked by the firewall rule defined on the perimeter gateway until the destination IP address set was expanded to include the destination NAT address.

    Q1. Why does the distributed firewall rule allow browser connections to the web server through the destination NAT address, when the rule explicitly defines web-sv-01a's IP address as the only valid destination?

Task 5: Review Distributed Firewall Log Entries

You review log entries that detail connections that are allowed or blocked by firewall rules.

1. Restore the web-sv-01a console window from the Windows task bar.

2. At the web-sv-01a command prompt, attempt to ping servers.

    - 10.1.20.11 (IP address of app-sv-01a)
    - 10.1.30.11 (IP address of db-sv-01a)

    Your ping should fail.

3. Press Ctrl+C to stop each `ping` command.

4. Press Ctrl+Alt to release the pointer and return to vSphere Web Client.

5. Point to the vSphere Web Client **Home** icon and select **Hosts and Clusters.**

6. Select the **web-sv-01a** VM in the Navigator pane, and identify the host where the VM is running.

    The host name appears in the **Summary** tab of the VM.

7. Minimize the browser window and restore the MTPuTTY application.

8. Double-click the ESXi host where the web-sv-01a VM resides in the MTPuTTY application.
9. Open the `dfwpktlogs.log` file with the vi text editor by using the `vi dfwpktlogs.log` command.

   The full path to open the log file is `vi /var/log/dfwpktlogs.log`.
10. Search for the `PASS` string in the log file.

    To search for the keyword `PASS`, you enter **`/PASS`** in the vi editor.

    Log entries describing connections that were allowed because of a firewall rule appear.
11. Search for the `DROP` string in the log file.

    Log entries describing connections that were dropped because of a firewall rule appear.
12. Press Esc and enter **`:q!`**to close the log file.

    Your prompt should return.
13. Restore the browser application.

Task 6: Restore a Saved Distributed Firewall Configuration

You restore the firewall configuration from a saved backup.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the Navigator pane, select **Firewall**.
3. In the middle pane, click the **Saved Configurations** tab.

   The configuration list contains several new entries that were autosaved by the system.
4. Click **Configuration** and click **General**.
5. Click the **Load saved configuration** icon.
6. In the Load Saved Configuration dialog box, scroll down and select the last autosaved configuration with today’s date and click **Load**.

   The oldest autosaved configuration was saved when Test Section was created, before new rules are defined.
7. When prompted to confirm, read the message and click **Yes**.
8. Click **Publish Changes** and wait for the update to complete.

Task 7: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Leave the MTPuTTY window open.
2. Leave the Command Prompt window open.
3. In the browser window, leave the **vSphere Web Client** tab open.
4. Leave the web-sv-01a console window open.

Lab 18 Using NSX Edge Firewall Rules to Control Network Traffic

Objective: Define NSX Edge firewall rules to restrict traffic to web servers

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Restrict Inbound Web Server Traffic to HTTP and HTTPS
3. Determine How the Firewall Rule Interacts with Other NSX Edge Features
4. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. On the student desktop, double-click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the MTPuTTY window is not open on the student desktop, open the MTPuTTY window.
   a. On the student desktop, double-click the **MTPuTTY** shortcut.
   b. In the MTPuTTY window, double-click the saved **Perimeter Gateway** session.

      172.20.11.3 is the IP address of the perimeter gateway.
   c. If prompted to confirm a PuTTY security alert, click **Yes**.
   d. Log in as admin and enter the password **`VMware1!VMware1!`**.
3. If the Firefox window is closed, double-click the **Firefox** icon on the student desktop.
4. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
5. When prompted, select the **Use Windows session authentication** check box and click **Login**.
6. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.
7. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.

Task 2: Restrict Inbound Web Server Traffic to HTTP and HTTPS

You configure a new firewall rule to restrict traffic destined for a web server to HTTP and HTTPS.

1. In the Navigator pane, select **NSX Edges**.
2. From the **NSX Manager** drop-down menu, select **172.20.10.42**.
3. In the edge list, double-click the **Perimeter Gateway** entry to manage that object.
4. In the middle pane, click the **Manage** tab and click **Firewall**.
5. In the firewall rules list, find the rule named Default Rule.
6. If necessary, use the horizontal scroll bar to uncover the Action column.
7. Point to the **Action** cell until a plus sign appears.
8. Click the plus sign to open a dialog box.
9. From the **Action** drop-down menu, select **Deny**.
10. Click **Log** and click **OK**.
11. Above the rule list, click **Publish Changes** and wait for the update to complete.
12. Open a new browser tab and go to https://10.1.10.11.

    10.1.10.11 is the IP address of the web-sv-01a VM.
13. Verify that the webpage cannot be displayed and close the browser tab.
14. On the Firewall configuration page, click the green plus sign to create a row in the rules table.

    The new row is highlighted.
15. Point to the **Name** cell and click the plus sign.
16. In the **Rule Name** text box, enter **`Allow-to-Web-Servers`** and click **OK**.
17. Point to the **Destination** cell and click the pencil icon.

    The Specify Destination dialog box opens.

18. Configure the destination settings.

    a. From the **Object Type** drop-down menu, select **IP Sets**.

    b. At the bottom, click the **New IP Set** link to open the Add IP Set dialog box.

Option	Action
Name	Enter `Local-Web-Servers`.
Description	Leave blank.
IP Addresses	Click the green plus sign, and enter `10.1.10.11` (IP address of web-sv-01a) in the text box.

    c. Click **OK** to close the Add IP Set dialog box.

    d. Click **OK** to close the Specify Destination window.

19. Point to the **Service** cell and click the pencil icon.

20. Configure the service settings.

    a. Enter `HTTP` in the **Filter** text box.

    b. In the Available Objects pane, select generic **HTTP** and **HTTPS** services.

    c. Click the right arrow to move **HTTP** and **HTTPS** to the Selected Objects list.

    d. Click **OK**.

21. Verify that **Accept** is selected from the **Actions** menu for the new rule.

22. Click **Publish Changes** and wait for the update to complete.

23. Open a new browser tab and go to https://10.1.10.11.

24. Verify that the webpage is displayed or that you are prompted with a certificate related warning, and close the browser tab.

Task 3: Determine How the Firewall Rule Interacts with Other NSX Edge Features

You determine how a firewall rule interacts with an existing destination NAT rule.

1. Open a new browser tab and go to https://172.20.11.7.

   172.20.11.7 is the load balancer's IP address.

2. Verify that the webpage is not displayed, and close the browser tab.

3. Return to vSphere Web Client.

   Q1. Because the virtual server for load balancing HTTP traffic was configured with the web-sv-01a web server as a member server, will the rule that you created allow HTTP connections to the virtual server IP address?

4. Open a new browser tab and go to https://172.20.11.5.

   172.20.11.5 is the destination NAT address of the web-sv-01a web server.

5. Verify that the webpage cannot be displayed, and close the browser tab.

   If the page does display, it is likely to be cached, so close the tab and reload the page to verify.

6. In vSphere Web Client, click the **Manage** tab and click **Grouping Objects**.

7. In the category panel, select **IP Sets**.

8. In the IP Set list, select the **Local-Web-Servers** entry.

9. Click the pencil icon to open the Edit IP Set dialog box.

   a. Click the green plus sign to add the IP address **`172.20.11.5`** in a new line.

   b. Click **OK**.

10. Open a new browser tab and go to https://172.20.11.5.

11. Verify that the webpage is displayed or that you are prompted with a certificate warning, and close the browser tab.

12. In vSphere Web Client, click the **Manage** tab and click **Firewall**.

13. In the rule list, select the **Allowed to Web Servers** rule.

14. Click the red X to delete the rule, and click **OK** when prompted to confirm.
15. Click **Publish Changes**.
16. Point to the **Default Rule Action** cell and click the plus sign.
17. From the **Action** drop-down menu, select **Accept** and disable the **Log** option**.**
18. Click **OK**.
19. Click **Publish Changes** and wait for the update to complete.

Task 4: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Leave the MTPuTTY window open.
2. Leave the Command Prompt window open.
3. At the top of the Navigator pane, click the **Networking & Security** left arrow.
4. In the browser window, leave the **vSphere Web Client** tab open.
5. Leave the web-sv-01a console window open.

Lab 19 Configuring and Using SpoofGuard and IP Discovery

Objective: Configure and test SpoofGuard, using VMware Tools as the IP discovery method

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Prepare the Infrastructure for SpoofGuard
3. Verify That the SpoofGuard Policy Is Operational
4. Configure SpoofGuard to Remove the Windows7-2 VM from the Approval List
5. Verify That the Windows7-2 VM Is No Longer Trusted
6. Verify That the Windows7-2 VM Is Trusted Again, and Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
2. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
3. When prompted, select the **Use Windows session authentication** check box and click **Login**.
4. Open the console window for the Windows7 VM.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.

   b. Expand the inventory tree and locate **Discovered virtual machine > Windows7**.

   c. Right-click **Windows7** and select **Power > Power On**.

   d. When the VM is completely powered on, click the **Summary** tab.

   e. Click the console thumbnail image.

   f. Press Ctrl+Alt to release the pointer.

   g. Return to vSphere Web Client.

5. Open the console window for the Windows7-2 VM.

   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.

   b. Expand the inventory tree and locate **Discovered virtual machine > Windows7**-2.

   c. Right-click **Windows7-2** and select **Power > Power On**.

   d. When the VM is completely powered on, click the **Summary** tab.

   e. Click the console thumbnail image.

   f. Press Ctrl+Alt to release the pointer.

   g. Return to vSphere Web Client.

Task 2: Prepare the Infrastructure for SpoofGuard

You deploy a SpoofGuard policy that automatically trusts IP addresses on first use. These addresses are learned through VMware Tools™.

1. In vSphere Web Client, point to the **Home** icon and select **Networking & Security**.
2. Select **SpoofGuard** in the Navigator pane.
3. Select the **Default Policy** in the middle pane, and click the pencil icon to edit the policy.
4. In the Edit Policy pop-up window, click **Enabled**.
5. Verify that **Automatically trust IP assignments on their first use** is selected.
6. Click **Finish** at the bottom of the window.
7. In the lower portion of the middle pane, verify that the **View** drop-down menu is set to **Active Virtual Nics** and that all running virtual machines in SA-Compute-01 are listed.
8. Verify that NSX is learning IP addresses through VMware Tools and not through DHCP or ARP snooping by clicking **Change** at the top of the middle pane.

   Neither DHCP nor ARP snooping is enabled, so NSX must be learning through VMware Tools.
9. Click **Cancel** to close the Global IP Detection Type pop-up window.

Task 3: Verify That the SpoofGuard Policy Is Operational

You verify that SpoofGuard is operational by performing pings and HTTP web browsing from the Windows7 and Windows7-2 VMs with the policy as is. You clear one of the VMs from the approval list and see that the VM is unable to perform the same activities afterward.

1. Click the **Windows7 VM Console** tab and go to **Home > Run**.
2. Enter `CMD` and press Enter.
3. At the command prompt, enter `ping 172.20.10.151` and press Enter.

   172.20.10.150 is the IP address for the Windows7-2 VM and should respond.
4. Click the **Windows7-2 VM Console** tab and go to **Home > Run**.
5. Enter `CMD` and press Enter.
6. At the command prompt, enter `ping 172.20.10.150` and press Enter.

   172.20.10.150 is the IP address for the Windows7 VM and should respond.
7. In the task bar of the Windows7 VM, click the browser icon and go to http://10.1.10.11.
8. When prompted by the Set Up Windows Internet Explorer 8 pop-up window, click **Ask me later**.

   10.1.10.11 is the address of web-sv-01a and should respond.
9. Click the **Windows7-2 VM Console** tab.
10. Click the browser icon and go to http://10.1.10.11.
11. When prompted by the Set Up Windows Internet Explorer 8 pop-up window, click **Ask me later**.

    10.1.10.11 is still the address of web-sv-01a and should respond.

Task 4: Configure SpoofGuard to Remove the Windows7-2 VM from the Approval List

You configure SpoofGuard so that the Windows7-2 VM is no longer on the Approval list and thus is not trusted.

1. Return to vSphere Web Client.
2. Select **SpoofGuard** in the Navigator pane, and click **Clear** next to the Windows7-2 VM (172.20.10.151) in the bottom of the middle pane.
3. Click **Publish Changes** at the top of the middle pane and wait for the publish operation to complete.
4. At the bottom of the middle pane, verify that Windows7-2 (172.20.10.151) is no longer in the list.

Task 5: Verify That the Windows7-2 VM Is No Longer Trusted

Using the administrator account, you log in to the Windows7 VM. You try to perform pings and web browsing to confirm that a virtual machine (Windows7-2) is no longer trusted.

The administrator user account can open the webpage and ping web-sv-01a VM, which is a part of the Compute cluster. However, the normal user account logged in to Windows7-2 cannot open the webpage and ping the web-sv-01a VM. This test confirms that the Identity Firewall functions as expected.

1. Click the **Windows7 VM Console** tab and go to **Home > Run**.
2. Enter **`CMD`** and press Enter.
3. At the command prompt, enter **`ping 172.20.10.151`** and press Enter.

   172.20.10.151 is the IP address for the Windows7-2 VM and should fail.
4. Click the **Windows7-2 VM Console** tab and go to **Home > Run**.
5. Enter **`CMD`** and press Enter.
6. At the command prompt, enter **`ping 172.20.10.150`** and press Enter.

   172.20.10.150 is the IP address for the Windows7 VM and should fail.
7. In the task bar of the Windows7 VM, click the browser icon and go to http://10.1.10.11.

   10.1.10.11 is the address of web-sv-01a and should respond.
8. Click the **Windows7-2 VM Console** tab, click the browser icon, and go to http://10.1.10.11.

   10.1.10.11 is still the address of web-sv-01a and should also fail.

   The Windows7-2 VM is no longer trusted as either a source or a destination of network activity.

Task 6: Verify That the Windows7-2 VM Is Trusted Again, and Clean Up for the Next Lab

You reapprove a virtual machine (Windows7-2), and you perform the previously denied actions, such as ping and web browsing, to verify that the virtual machine is trusted again.

1. Return to vSphere Web Client.
2. In the SpoofGuard bottom pane list of IP addresses to approve, select **Virtual Nics IP Required Approval** from the **View** drop-down menu.

   Only the Windows7-2 VM should appear in the list.
3. Click the **Approve** link in the Action Column of the list.
4. Click **Publish Changes** at the top of the middle pane and wait for the publish operation to complete.
5. Select **Active Virtual Nics** from the **View** drop-down menu.

   The Windows7-2 VM should return to the whole list.
6. Return to the Windows7-2 console widow and refresh the webpage.

   The web-sv-01a web page should respond.
7. Click the Command Prompt window icon in the task bar of the Windows 7-2 console.
8. Click in the Command Prompt window, press the up arrow to recall the `ping` command, and press Enter.

   The pings to the Windows7 VM should be successful again.
9. Return to the Windows7 console window.
10. Click the Command Prompt window icon in the task bar of the Windows7 console
11. Click in the Command Prompt window, press the up arrow to recall the `ping` command, and press enter.

    The pings to the Windows7-2 VM should be successful again.
12. Close the console tabs for the Windows7 and Windows7-2 VMs.
13. In the browser window, leave the **vSphere Web Client** tab open.

Lab 20 Using NSX Service Composer

Objective: Define NSX Service Composer security groups and security policies

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Create a Security Group
3. Create a Security Policy
4. Verify the Policy Functionality Before the Virus Is Found
5. Verify the Policy Functionality After the Virus Is Found
6. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
    a. On the student desktop, double-click the **Command Prompt** shortcut.
    b. Move the Command Prompt window to a convenient place on the desktop.
2. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
3. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
4. When prompted, select the **Use Windows session authentication** check box and click **Login**.
5. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.

Task 2: Create a Security Group

You create a security group that includes web servers in the Compute clusters.

1. In the Navigator pane, select **Service Composer**.
2. Verify that **172.20.10.42** is selected from the **NSX Manager** drop-down menu.
3. In the middle pane, click the **Security Groups** tab.
4. Click the **New Security Group** icon to open the New Security Group dialog box.
5. On the Name and description page, enter **`Quarantine-Group`** in the **Name** text box and click **Next**.
6. In the Criteria Details section of the Define dynamic membership page, select **VM Name** from the first drop-down menu.
7. Leave **Contains** selected from the second drop-down menu.
8. Enter **`virus`** in the last text box.
9. Click **Next**.
10. On the Select objects to include page, click **Next**.
11. On the Select objects to exclude page, select **Distributed Port Group** from the **Object Type** drop-down menu.
12. In the Available Objects pane, select **pg-SA-Management** and click the right arrow to add it to the Selected Objects list.
13. Click **Next**.
14. On the Ready to complete page, review the settings and click **Finish.**

Task 3: Create a Security Policy

You configure a security policy to isolate ports in the security group.

1. In the middle pane, click the **Security Policies** tab.
2. Click the **Create Security Policy** icon.

   The New Security Policy window appears.
3. On the Name and description page, enter `Isolate-Compromised-VMs` in the **Name** text box.
4. Leave all other settings at their default value and click **Next**.
5. On the Guest Introspection Services page, click **Next**.
6. On the Firewall Rules page, click the green plus sign.

   The New Firewall Rule dialog box appears.
7. In the **Name** text box, enter `Block-all-Traffic`.
8. Select **Block** for Action.
9. For Source, click the **Change** link.

   The Block all Traffic - Select Source dialog box appears.
10. For Select security groups to add, select **Any.**
11. Click **OK**.
12. For Destination, click the **Change** link.

    The Block all Traffic - Select Destination dialog box appears.
13. For Select security groups to add, leave **Policy's Security Groups** selected.
14. Leave all other settings at their default value and click **OK**.
15. Click **OK**.
16. Click **Next**.
17. On the Network Introspection Services page, click **Next**.
18. On the Ready to complete page, click **Finish**.
19. Select the **Isolate-Compromised-VMs** entry, and select **Apply Policy** from the **Actions** menu.

    The Isolate Compromised VMs - Apply Policy to Security Groups dialog box opens.
20. Select the **Quarantine Group** check box and click **OK**.

Task 4: Verify the Policy Functionality Before the Virus Is Found

You verify the security policy configuration before the virus is found.

1. At the student desktop command prompt, ping the web-sv-01a VM.

   ```
   ping -t 10.1.10.11
   ```

   The pings should be received.

2. Return to vSphere Web Client.

3. Ensure that **Service Composer** is selected in the Navigator pane.

4. Click the **Canvas** tab in the middle pane.

   The Quarantine group is represented as a box. A security policy is associated with the Quarantine group. You can identify the name of the security policy by clicking the icon in the top-right corner of the box. The number of VMs added to the group is zero.

5. Point to the **Home** icon and select **VMs and Templates**.

6. In the `Discovered virtual machines` folder, select the **web-sv-01a** VM in the Navigator pane.

7. Click the **Monitor** tab in the middle pane.

8. Click the **Service Composer** tab.

9. Verify that no security services are associated with the VM by selecting **Guest Introspection Services, Firewall Rules**, and **Network Introspection Services** individually.

Task 5: Verify the Policy Functionality After the Virus Is Found

You verify the security policy configuration after a virus is found in the web-sv-01a VM.

1. Ensure that **web-sv-01a** is selected in the Navigator pane.

2. Select **Rename** from the **Actions** menu.

3. At the end of the VM's name, enter **`_virus`**.

   The new VM name should be web-sv-01a_virus.

4. Click **OK**.

5. Maximize the Command Prompt window, and determine whether the ping requests time out.

6. Return to vSphere Web Client, and click the refresh icon next to the user name.

7. Ensure that the **web-sv-01a_virus** VM is selected in the Navigator pane.

8. Click **Monitor** and click **Service Composer**.

9. Select **Firewall Rules** in the middle pane, and verify that the Block-all-Traffic firewall policy is applied to the VM.
10. Point to the **Home** icon and select **Networking & Security**.
11. Select **Service Composer** in the Navigator pane.
12. Click the **Canvas** tab.

    The Quarantine group has one VM associated with it.
13. Click the **VM** icon at the top of the Quarantine Group box, and verify that the name of the VM is web-sv-01_virus.

Task 6: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Point to the **Home** icon and select **VM and Templates**.
2. In the Navigator pane, right-click **web-sv-01a_virus** and select **Rename**.
3. Delete _virus from the VM's name and click **OK**.

   The VM's name is now web-sv-01a.
4. Maximize the Command Prompt window, and verify that the pings are successful.
5. Press Ctrl+C to stop the `ping` command.
6. Leave the Command Prompt window open.
7. In the browser window, leave the **vSphere Web Client** tab open.
8. Leave the web-sv-01a console window open.

Lab 21 Configuring an Identity-Aware Firewall

Objective: Configure an identity-aware firewall

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Prepare the Infrastructure for an Identity-Aware Firewall
3. Add an Active Directory Domain to the NSX Manager Instance
4. Configure Identity-Aware Firewall Rules
5. Verify the Identity-Aware Firewall Configuration
6. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
    a. On the student desktop, double-click the **Command Prompt** shortcut.
    b. Move the Command Prompt window to a convenient place on the desktop.
2. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
3. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
4. When prompted, select the **Use Windows session authentication** check box and click **Login**.

5. Open the console window for the Windows 7 VM.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and locate **Discovered virtual machine > Windows7**.
   c. Click the **Launch Console** link under the console thumbnail image.
   d. Click the console thumbnail image.
   e. Press Ctrl+Alt to release the pointer.
   f. Return to vSphere Web Client.
6. In the MTPuTTY window, double-click the saved **Perimeter Gateway** session to connect to it.

Task 2: Prepare the Infrastructure for an Identity-Aware Firewall

You deploy Guest Introspection and enable Activity Monitoring for the Compute cluster. These features are prerequisites for configuring the identity-aware firewall.

1. In vSphere Web Client, point to the **Home** icon and select **Networking & Security**.
2. Select the **Installation and Upgrade** in the Navigator pane.
3. Click the **Service Deployments** tab in the middle pane.
4. In the Network & Security Service Deployments pane, click the green plus sign.

   The Deploy Network & Security Services window appears.
5. On the Select services & schedule page, select the **Guest Introspection** check box and click **Next**.
6. Ensure that **SA-Datacenter** is selected from the **Datacenter** drop-down menu.
7. Select the **SA-Compute-01** check box and click **Next**.
8. On the Select storage and Management Network page, enter configuration details.
   - Datastore: SA-Shared-01-Remote
   - Network: pg-SA-Management
9. Under IP Assignment, click the **Change** link.

   The Select IP Assignment mode window appears.
10. Select **Use IP Pool**, select **Controller-Pool**, and click **OK**.
11. Click **Next**.
12. On the Ready to complete page, click **Finish**.

    You can configure Activity Monitoring for the Compute cluster while Guest Introspection is deployed.

13. In the Navigator pane, select **Service Composer**.
14. Click the **Security Groups** tab in the middle pane.
15. Right-click the **Activity Monitoring Data Collection** group and select **Edit Security Group**.

    The Edit Security Group window appears.
16. In the left pane, select **Select objects to include**.
17. Select **Cluster** from the **Object Type** drop-down menu.
18. In the Available Objects list, select **SA-Compute-01** and click the right blue arrow to move it to the Selected Objects list.
19. Click **Finish**.
20. Select **Installation and Upgrade** in the Navigator pane.
21. Verify that the deployment of Guest Introspection is complete and the installation status appears as Succeeded.

Task 3: Add an Active Directory Domain to the NSX Manager Instance

You add an Active Directory domain to the NSX Manager instance for configuring an identity-aware firewall.

1. Select **Users and Domains** in the left pane.
2. Click the **Domains** tab in the middle pane**.**
3. Click the green plus sign to add an Active Directory domain.
4. On the Name page, enter **`vclass.local`** in the **Domain Name** text box.
5. Enter **`vclass`** in the **NetBIOS Name** text box and click **Next**.
6. On the LDAP Options page, enter configuration details.
    - Server: dc.vclass.local
    - Username: administrator
    - Password: VMware1!
7. Leave all other default settings and click **Next**.
8. On the Security Event Log Access page, leave the default settings and click **Next**.
9. Click **Finish** on the Ready to complete page.

Task 4: Configure Identity-Aware Firewall Rules

You configure two rules in the Default section of the distributed firewall. One rule allows SSH connections to the win-sv-01a VM for domain group AD-SSH. This group includes the administrator user accounts. The other rule blocks the SSH connection to the win-sv-01a VM for all other users.

1. In the Navigator pane, select **Groups and Tags**.
2. In the middle pane, click the **Security Group** tab
3. Click the green plus sign to add a group.
4. In the Name and description page, enter `Admins-Web` in the **Name** text box and click **Next**.
5. In the Define dynamic membership page, click **Next**.
6. In the Select objects to include page, select **Directory Group** from the **Object Type** drop-down menu.
7. In the Available Objects list, select **Domain Admins** and click the blue right arrow to move it to the Selected Objects list.
8. Click **Next**.
9. On the Select Objects to exclude page, click **Finish**.
10. In the Navigator pane, select **Firewall**.
11. If necessary, use the horizontal scroll bar to uncover the icons on the far-right side of the **Default Section** entry.
12. Click the green plus sign on the same line as Default Section Layer3 to create a rule.
13. Find the new rule entry, point to the **Name** cell, and click the pencil icon.
14. In the **Rule Name** text box, enter `Admins-Allowed-to-Web` and click **Save**.
15. Point to the **Source** cell and click the pencil icon to open the Specify Source configuration window.
16. From the **Object Type** drop-down menu, select **Security Group**.
17. In the Available Objects list, select **Admins-Web** and click the blue right arrow to move it to the Selected Objects list.
18. Click **OK**.
19. Point to the **Destination** cell and click the pencil icon to open the Specify Destination configuration page.
20. From the **Object Type** drop-down menu, select **Cluster**.

21. In the Available Objects list, select **SA-Compute-01** object and click the blue right arrow to move it into the Selected Objects list.

22. Click **OK**.

23. Point to the **Services** cell and click the pencil icon to open the Specify Service configuration page.

24. In the **Filter** box, enter **`http`** and press Enter.

25. In the Available Objects list, select **HTTP** and **HTTPS** and click the blue right arrow to move them to the Selected Objects list.

26. Click **OK**.

27. Point to the rule number of Admins-Allowed-to-Web, and right-click and select **Add Below** from the drop-down menu.

    This rule must appear below the rule that you created.

28. Point to the **Name** cell and click the pencil icon.

29. In the **Rule Name** text box, enter **`Blocked-Web-for-Normal-Users`** and click **OK**.

30. Leave **any** as the value in the **Source** cell.

31. Point to the **Destination** cell and click the pencil icon to open the pop-up configuration page.

32. From the **Object Type** drop-down menu, select **Cluster**.

33. In the Available Objects list, select **SA-Compute-01** and click the blue right arrow to move it into the Selected Objects list.

34. Click **OK**.

35. Point to the **Services** cell and click the pencil icon to open the pop-up configuration page.

36. In the **Filter** box, enter **`http`** and press Enter.

37. In the Available Objects list, select **HTTP** and **HTTPS** and click the blue right arrow to move them to the Selected Objects list.

38. Click **OK**.

39. Point to the **Action** cell and click the pencil icon to open the pop-up configuration page.

40. From the **Actions** drop-down menu, select **Block**.

41. Click **Save**.

42. Click **Publish Changes** at the top of the middle pane.

Task 5: Verify the Identity-Aware Firewall Configuration

Using two accounts (normalusera and administrator), you use a web browser to verify that the identity-aware firewall configurations are functioning as expected.

1. Click the **Windows7** VM console tab in the browser.
2. In the console browser window, go to http://10.1.10.11.
3. Wait for the page to display and then select **Home > Shutdown > Switch User** in the Windows7 VM.
4. Click **Other User** and log in with vclass\normalusera and password VMware1!.

   vclass\normalusera is the normal user for Windows VM.
5. Click **Start > Run**, enter **`CMD`**, and press Enter.
6. Enter **`whoami`** and press **Enter**.

   The response confirms that you are logged in as vclass\normalusera, and thus you cannot connect to the web server.
7. In the task bar of the Windows7 VM, click the browser icon.
8. In the browser window, go to http://10.1.10.11.
9. When prompted by the Set Up Windows Internet Explorer 8 pop-up window, click **Ask me later**.
10. Wait for the page to fail to display, and close the console tab for Windows7.
11. In the student desktop browser, open a new tab and enter **`https://10.1.10.11`** to connect to web-sv-01a.
12. Verify that either the page opens or you receive a warning about the website's certificate.
13. In the task bar of the student desktop VM, click the Command Prompt window icon.
14. Enter **`whoami`** and press Enter.

    The response confirms that you are logged in as vclass\administrator, and thus you can connect to the web server.

Task 6: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Close the console window for the Windows7 VM.
2. Close the tab for the 10.1.10.11 web server.
3. Return to vSphere Web Client and select **Home > Networking & Security**.
4. In the Navigator pane, select **Firewall**.
5. In the middle pane, click the **Load saved configuration** icon.
6. In the Load Saved Configuration pop-up window, scroll to the bottom, select the last autosaved configuration, and click **Load**.
7. In the warning message about replacing the current configuration, click **Yes**.
8. When the page is loaded, click **Publish Changes** and wait for the publish operation to complete.
9. In the browser window, leave the **vSphere Web Client** tab open.

Lab 22 Micro-Segmentation with Application Rule Manager

Objective: Collect network activity, and use Application Rule Manager to create firewall rules for micro-segmenting the web, application, and database network tiers

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Create a Session and Capture Traffic Flows
3. Analyze the Traffic Flow Session Results
4. Publish and Analyze the Application Rule Manager Recommendations
5. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. On the student desktop, double-click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
3. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
4. When prompted, select the **Use Windows session authentication** check box and click **Login**.

5. Open the console window for the Windows7 VM.

    a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.

    b. Expand the inventory tree and locate **Discovered virtual machine > Windows7**.

    c. Right-click **Windows7** and select **Power > Power On**.

    d. When the VM is completely powered on, click the **Summary** tab.

    e. Click the **Launch Console** link under the console thumbnail image.

    f. Click the console thumbnail image.

    g. Press Ctrl+Alt to release the pointer.

    h. Return to vSphere Web Client.

6. In the MTPuTTY window, double-click the saved **Perimeter Gateway** session to connect to it.

7. Log in as user admin with the password VMware1!VMware1!.

Task 2: Create a Session and Capture Traffic Flows

You use `ping` and web browsing to capture traffic generated for Flow Monitoring to analyze.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.

2. Select **Flow Monitoring** in the Navigator pane.

3. Click the **Application Rule Manager** tab in the middle pane.

4. Click **Start New Session**.

5. In the Start a New Session window, enter **`Microsegment-Web-App`** in the **Session Name** text box.

6. Leave the Object Type as virtual machines and double-click the machines to move them from the Available Objects list to the Selected Objects list.

    - app-sv-01a

    - db-sv-01a

    - web-sv-01a

    - web-sv-02a

7. Verify that all four virtual machines are selected and click **OK**.
8. Open the web-sv-01 console tab and ping selected addresses.
   - 10.1.10.12
   - 10.1.20.11
   - 10.1.30.11
9. After each ping runs for a few minutes, press Ctrl+C to stop each ping.
10. Open a new tab in the browser, enter **`https://10.1.10.11`**, and wait for the webpage to display.
11. On the same tab, replace the IP address with https://10.1.10.12 and press Enter.
12. When prompted that your connection is not secure, click **Advanced** and click **Add Exception**.
13. In the Add Exception pop-up window, click **Confirm Security Exception**.
14. On the same tab, replace the IP address with https://172.20.11.5 and press Enter.
15. Return to the Application Rule Manager Collecting Data session and click the **Stop** link below the Collecting Data object in the middle pane.

Task 3: Analyze the Traffic Flow Session Results

You analyze the traffic flows captured and the various categories of the different views.

1. Wait for the **Stop** link to change to **Analyze**, and click **Analyze.**

   The middle pane displays recommended firewall rules for the analyzed traffic flows.
2. After viewing the generated firewall rules, click the **View Flows** tab to see what traffic flows the rules were created from.
3. At the far right of the View Flows pane, click **Processed View** and select **Consolidated View**.

   Q1. What is the difference between the two views?

4. At the top of the middle pane, click the **Security Group(s)** link.
5. Click any line in the list and click the pencil icon to edit.

   Q2. What actions can you take on the selected security object?

6. Click **step 3 Select objects to include** in the Edit Security Group pop-up window.

   Q3. What objects are already in the Selected Objects list?

   Q4. Where did the objects in the Selected Objects list come from?

7. Click **Cancel** to leave the Edit Security Group window.
8. Click **OK** to leave the Security Group window.

Task 4: Publish and Analyze the Application Rule Manager Recommendations

After capturing and analyzing network traffic, you review the recommended firewall rules created by Application Rule Manager.

1. Below the **Firewall Rules** tab in the middle pane, click the **Publish** link.
2. Enter **`ARM-Section`** in the **Section Name** text box of the Firewall Publish pop-up window.
3. Leave all other options as set and click **OK**.
4. Select **Firewall** in the Navigator pane.
5. Locate **ARM-Section** in the Firewall General Rules list, and click the pointer icon to expand this section.

   Q1. Are these the same entries you saw before in the Application Rule Manager of the Flow Monitoring results?

Task 5: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. In the Firewall pane, locate **ARM-Section** and click the red X to delete the section.
2. Click **Yes** in the Remove rule section pop-up window.
3. Click **Publish Changes** in the top left of the middle pane.
4. In the browser window, leave the **vSphere Web Client** tab open.
5. Leave the web-sv-01a console window open.

Lab 23 Guest Introspection and Endpoint Monitoring

Objective: Use Guest Introspection to capture actions performed by users in virtual machines

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Prepare the Infrastructure for Endpoint Monitoring
3. Use Login, Ping, Web Browsing, and PuTTY to Create Data to Collect
4. Analyze the Data Collection Results
5. Clean Up for the Next Lab

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If a Command Prompt window is not open on the student desktop, open the window.
   a. On the student desktop, double-click the **Command Prompt** shortcut.
   b. Move the Command Prompt window to a convenient place on the desktop.
2. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
3. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
4. When prompted, select the **Use Windows session authentication** check box and click **Login**.

Task 2: Prepare the Infrastructure for Endpoint Monitoring

You create some objects and enable Endpoint Monitoring for the Compute cluster.

In lab 21, you deployed Guest Introspection services to the SA-Compute cluster.

1. In vSphere Web Client, point to the **Home** icon and select **Networking & Security**.
2. Select **Groups and Tags** in the Navigator pane.
3. Verify that **172.20.10.42** is selected from the **NSX Manager** drop-down menu.
4. Click the **Security Group** tab in the middle pane.
5. In the Groups and Tags Security Group pane, click the green plus sign.

   The Add Security Group window appears.
6. On the Name and description page, enter **`Windows-VMs`** and click **Next**.
7. On the Define dynamic membership page, click **Next**.
8. On the Select objects to include page, select **Virtual Machine** from the **Object Type** drop-down menu and Shift-select **Windows7** and **Windows7-2**.
9. Using the right blue arrow, move the virtual machines to the Selected Objects list and click **Next**.
10. On the Select objects to exclude page, click **Finish**.
11. In the Navigator pane, select **Endpoint Monitoring**, and click the **Start Collecting Data** link on the far right of the middle pane.
12. In the Start Data Collection for Security Groups pop-up window, click the **Select your security group here** link.
13. In the Select Security Group pop-up window, select **Windows-VMs** and click **OK**.
14. In the Start Data Collection for Security Groups pop-up window, toggle **Switch data collection ON or OFF** to **ON** and click **OK**.

Task 3: Use Login, Ping, Web Browsing, and PuTTY to Create Data to Collect

You log in to two Windows VMs, ping between the VMs, browse a website, and use SSH to connect to another machine in order to create network activity for Endpoint Monitoring data collection.

1. If the Windows7 VM console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the inventory tree and select **Discovered virtual machine** > **Windows7**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name vclass\administrator and the password VMware1!.
2. On the desktop, open **Home > Run**, and enter **`CMD`**, and press Enter.
3. At the command prompt, enter **`ping 172.20.10.151`** and press Enter.

   The pings to the Windows7-2 VM should be successful.
4. On the desktop, click the browser icon in the task bar.
5. In the browser window, go to http://10.1.10.11.

   The webpage of web-sv-01a should appear.
6. Go to **Home > Computer** and double-click **Local Disk (C:)**.
7. Double-click the folder `putty` folder, and double-click the `putty` program.
8. Enter **`172.20.10.53`** in the **Host and Name** text box.
9. In the PuTTY Security Alert pop-up window, click **Yes**.
10. Log in to the remote system with user name root and password VMware1!.
11. At the command prompt, enter **`exit`** and press Enter.
12. If the Windows7-2 VM console window is not open, open the console window.
    a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
    b. Expand the inventory tree and select **Discovered virtual machine** > **Windows7**.
    c. Click the **Summary** tab.
    d. Click the console thumbnail image.
    e. Log in with the user name vclass\normalusera and the password VMware1!.

13. On the desktop, open **Home** > **Run**, enter **`CMD`**, and press Enter.

14. At the command prompt, enter **`ping 172.20.10.150`** and press Enter.

    The pings to the Windows7 VM should be successful.

15. In the desktop, click the browser icon in the task bar.

16. In the browser window, go to http://10.1.10.12.

    The webpage of web-sv-02a should appear.

17. Go to **Home** > **Computer** and double-click **Local Disk (C:)**.

18. Double-click the folder `putty` folder, and double-click the `putty` program.

19. Enter **`10.1.10.12`** in the **Host and Name** text box.

20. In the PuTTY Security Alert pop-up window, click **Yes**.

21. Log in to the remote system with user name root and password VMware1!.

22. At the command prompt, enter **`exit`** and press Enter.

Task 4: Analyze the Data Collection Results

You return to Endpoint Monitoring and analyze the VM flows, process flows, and AD user flows that were collected as a result of task 3.

1. Point to the **Home** icon and select **Networking & Security**.

2. Select **Endpoint Monitoring** in the Navigator pane.

3. In the middle pane, review the information on the **Summary** tab.

    Q1. In the Virtual Machines and Processes section, how many virtual machines are running?

    Q2. In the Virtual Machines and Processes section, how many processes are generating traffic?

    a. Click the number in the Processes Generating Traffic section.

    Q3. What happens when you click the number?

b. Click the **VM Flows** tab.

Q4. Which virtual machines are listed?

c. In the lower portion of the middle pane, double-click the blue round object.

Q5. What happens when you double-click the object?

d. Click **Close** in the VM Details window.

4. In the middle pane, review the information on the **AD User Flows** tab.

Q6. How many and which users are listed?

5. In the lower portion of the middle pane, click the entry in the Login Time Column.

Q7. What happens when you click the entry?

6. Click **Close** in the User Flows Details pop-up window.
7. In the Endpoint Monitoring pane, click the **Stop Collecting Data** link on the far right.
8. Click **Yes** in the Stop Collecting Data confirmation pop-up window.

Task 5: Clean Up for the Next Lab

You perform these actions to prepare for the next lab.

1. Close the console windows for the Windows7 and Windows7-2 VMs.
2. In the browser window, leave the **vSphere Web Client** tab open.

Lab 24 Configuring the Cross-vCenter NSX Feature

Objective: Configure the cross-vCenter NSX feature, and use universal objects such as the universal logical switch and the universal distributed firewall

In this lab, you perform the following tasks:

1. Prepare for the Lab
2. Verify the Configuration of the NSX Manager Instances
3. Configure Primary and Secondary Roles for the NSX Manager Instances
4. Configure the Universal Segment ID Pool and the Universal Transport Zone
5. Create a Universal Logical Switch, and Connect the Web Servers
6. Reconfigure the IP Address of the web-sv-01b VM, and Verify L2 Connectivity Between the VMs
7. Configure the Universal Firewall Policy

Task 1: Prepare for the Lab

You perform these actions to prepare for the lab if you have closed windows or logged out of vSphere Web Client.

1. If the Firefox window is closed, click the **Firefox** icon in the task bar of the student desktop.
2. If you are not logged in to vSphere Web Client, click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark in the browser window.
3. When prompted, select the **Use Windows session authentication** check box and click **Login**.
4. If the web-sv-01a console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the Site-A-Datacenter inventory tree and select **Discovered virtual machine** > **web-sv-01a**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.
5. If the web-sv-01b console window is not open, open the console window.
   a. Point to the vSphere Web Client **Home** icon and select **VMs and Templates**.
   b. Expand the Site-B-Datacenter inventory tree and select **Discovered virtual machine** > **web-sv-01b**.
   c. Click the **Summary** tab.
   d. Click the console thumbnail image.
   e. Log in with the user name root and the password VMware1!.
   f. Press Ctrl+Alt to release the pointer.
   g. Click the **vSphere Web Client** tab in the browser.

Task 2: Verify the Configuration of the NSX Manager Instances

You verify the segment ID pools and the IDs of the NSX Manager instances. The cross-vCenter NSX feature does not work properly if the segment ID pools and IDs overlap.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the Navigator pane, select **NSX Home** and click the **Summary** tab.
3. In the middle pane, select **172.20.10.42**.

   172.20.10.42 is the IP address of nsxmgr-a.
4. Record the ID value. __________
5. In the middle pane, select **172.20.110.43**.

   172.20.110.43 is the IP address of nsxmgr-b.
6. Record the ID value. __________

   The ID values of the two NSX Manager instances must be different.
7. In the Navigator pane, select **Installation and Upgrade**.
8. Click the **Logical Network Preparation** tab.
9. From the **NSX Manager** drop-down menu, select **172.20.10.42**.
10. Click the **Segment ID** tab.
11. Record the **Segment ID pool** value. __________
12. From the **NSX Manager** drop-down menu, select **172.20.110.43**.
13. From the **Segment ID** tab, record the **Segment ID pool** value. __________

    The **Segment ID pool** values must not overlap for the two NSX Manager instances.

Task 3: Configure Primary and Secondary Roles for the NSX Manager Instances

You promote one of the NSX Manager instances to the primary role. After the NSX Manager instance is promoted, you register the other NSX Manager instance as secondary.

1. With **Installation and Upgrade** selected in the left pane, click the **Management** tab in the middle pane.
2. In the NSX Managers pane, ensure that the IP address of nsxmgr-a **172.20.10.42** is selected.
3. Select **Assign Primary Role** from the **Actions** menu.
4. Click **Yes** to confirm.
5. Verify that the role of nsxmgr-a is Primary and nsxmgr-b is standalone.

6. Select **172.20.10.42**.
7. Select **Add Secondary NSX Manager** from the **Actions** menu.
8. Verify that the IP address of nsxmgr-b **172.20.110.43** is selected is from the **NSX Manager** drop-down menu.
9. Enter the user name **`admin`**, and enter **`VMware1!`** in the **Password** and **Confirm password** text boxes.
10. Click **OK**.
11. When the Trust Certificate message appears, click **Yes** to proceed with this certificate.
12. Wait for a minute, and click the **Refresh** icon in vSphere Web Client.

    The status of all the NSX Controller nodes should be Connected (green check mark) before you proceed to the next task. nsxmgr-a and nsxmgr-b use the same NSX Controller node.

Task 4: Configure the Universal Segment ID Pool and the Universal Transport Zone

You configure the universal segment ID pool and the universal transport zone for using universal objects such as universal logical switches.

1. With **Installation and Upgrade** selected in the Navigator pane, click the **Logical Network Preparation** tab in the middle pane.
2. From the **NSX Manager** drop-down menu, select **172.20.10.42 (Role: Primary)**.
3. Click the **Segment ID** tab.
4. Click **Edit**.

    The Edit Segments and Multicast Address Allocation window appears.
5. In the Universal Segment ID pool and Multicast range pane, enter **`7000-7999`** in the **Universal Segment ID pool** text box.
6. Click **OK**.
7. Click the **Transport Zones** tab in the middle pane.
8. Click the green plus sign.
9. Select the **Mark this object for Universal Synchronization** check box.
10. In the **Name** text box, enter **`Universal-Transport-Zone`**.
11. Leave the replication mode as **Unicast**.
12. In the Selects clusters that will be part of the Transport Zone section, select the check boxes for both the **SA-Compute-01** and the **SA-Management** clusters.

13. Click **OK**.
14. From the **NSX Manager** drop-down menu, select **172.20.110.43 (Role: Secondary)**.
15. Click the **Transport Zones** tab.

    The universal transport zone is already replicated to the secondary NSX Manager instance.
16. Select **Universal-Transport-Zone**, click **Actions**, and select **Connect Clusters**.
17. Select the **SB-Management** check box.
18. Click **OK**.

Task 5: Create a Universal Logical Switch, and Connect the Web Servers

You create a universal logical switch to extend layer connectivity between workloads running on hosts managed by different vCenter Server systems.

1. Select **Logical Switches** in the Navigator pane.
2. From the **NSX Manager** drop-down menu, select **172.20.10.42 (Role: Primary)**.
3. Click the green plus sign to create a logical switch.
4. In the **Name** text box, enter **`Universal-Web-Tier`**.
5. For Transport Zone, click the **Change** link.
6. Select **Universal Transport Zone** and click **OK**.
7. In the New Logical Switch window, click **OK**.
8. In vSphere Web Client, point to the **Home** icon and select **Networking**.
9. Under the dvs-SA-Datacenter distributed switch, select the port group with SID 7000 and Universal-Web-Tier in the name.
10. Right-click the port group and select **Edit Settings**.
11. In the navigation pane of the Edit Settings pop-up window, select **Teaming and Failover**.
12. Use the blue up and down arrows to place **Uplink 3** in the Active Uplinks list and uplinks 1, 2, and 4 in the Unused Uplinks list.
13. Repeat steps 9 through 12 for the dvs-SB-Datacenter distributed switch port group with SID 7000 and Universal-Web-Tier in the name.
14. Perform steps 10-12 for the VTEP port group whose name should be similar to vxw-vnknicPg-dvs-### in both Site A and Site B.
15. In vSphere Web Client, point to the **Home** icon and select **Networking & Security**.
16. In the Navigator pane, select **Logical Switches**.

17. From the logical switches list, select **Universal-Web-Tier**.
18. Click **Actions** and select **Add VM**.

    The Universal-Web-Tier - Add Virtual Machines window appears.
19. In the Available Objects list, select **web-sv-01a** and **web-sv-02a** and click the right arrow to move them to the Selected Objects list.
20. Click **Next**.
21. Select the check box next to **web-sv-01a - Network adapter 1 (Web-Tier)** and **web-sv-02a - Network adapter 1 (Web-Tier)** and click **Next**.
22. Click **Finish**.
23. From the **NSX Manager** drop-down menu, select **172.20.110.43 (Role: Secondary)**.
24. Repeat steps 17 through 22 for the web-sv-01b VM in the remote vCenter Server inventory.

Task 6: Reconfigure the IP Address of the web-sv-01b VM, and Verify L2 Connectivity Between the VMs

You reconfigure the IP address of the web-sv-01b VM to be on the same subnet as the web-sv-01a VM.

1. Restore the web-sv-01b console window from the Windows task bar.
2. Change the IP address of the virtual machine.

    ```
    ifconfig eth0 10.1.10.14 netmask 255.255.255.0
    ```
3. Run the `ping 10.1.10.11` command to ping the web-sv-01a virtual machine.
4. Verify that `ping` gets a response.

    The two virtual machines are running on different hosts, on different subnets managed by different vCenter Server systems. Using universal logical switches, you can achieve layer 2 connectivity between the virtual machines.
5. Leave the `ping` command running on the web-sv-01b virtual machine.
6. Click the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** tab in the browser window.
7. Point to **Home** and select **Hosts and Clusters**.
8. Select the **web-sv-01a** virtual machine in SA-Datacenter.
9. Select **Rename** from the **Actions** menu.
10. Enter **`_SiteA`** at the end of the virtual machine’s name.

    The virtual machine name should be web-sv-01a_SiteA.
11. Click **OK**.

12. Select **Migrate** from the **Actions** menu.
13. Select the **Change both compute resource and storage** check box and click **Next**.
14. Expand **SB-Datacenter** and expand **SB-Management**.
15. Select the host **esxi-b-01** of SB-Datacenter.
16. Click **Next**.
17. Select **SB-Shared-01-Remote** in the Select storage window and click **Next**.
18. Select the **Discovered virtual machine** folder and click **Next**.
19. From the **Destination Network** drop-down menu, select the logical switch that includes "universalwire" in its name.
20. Click **Next**.
21. On the Select vMotion priority page, click **Next**.
22. On the Ready to complete page, click **Finish**.
23. Restore the web-sv-01b console window from the Windows task bar.
24. Verify that `ping` is still getting a response.
25. Return to the **vSphere Web Client** tab in the browser.
26. Click the refresh icon to refresh the vSphere Web Client view.
27. Verify that web-sv-01a_SiteA is moved to the host in Site-B-Datacenter.

    You performed a live migration of a virtual machine from one vCenter Server system to another without causing outage and without the need to change the IP address of the virtual machine.
28. Point to the **Home** icon and select **Networking & Security**.

Task 7: Configure the Universal Firewall Policy

You configure the universal firewall policy on the primary NSX Manager instance and confirm that the policy is replicated to the secondary NSX Manager instance.

The cross-vCenter NSX feature enables an administrator to configure security policies only once, and those policies follow the VMs as they are moved from one part of the infrastructure to another.

1. Point to the vSphere Web Client **Home** icon and select **Networking & Security**.
2. In the Navigator pane, select **Firewall**.
3. From the **NSX Manager** drop-down menu, select **172.20.10.42 (Role: Primary)** (the primary NSX Manager instance).

4. Click any folder icon to create a section.

   If necessary, scroll to the right to view the folder icon.

5. Enter **`Universal Section`** as the section name.
6. Select the **Mark this section for Universal Synchronization** check box.
7. Click **OK**.
8. Click **Publish Changes**.
9. In the Universal Section row, scroll to the right and click the green plus sign.
10. Expand **Universal Section** and select the new rule.
11. Point to the **Name** cell and click the pencil icon in the cell.
12. In the **Rule Name** text box, enter **`web-sv-01a`** and click **OK**.
13. Point to the **Destination** cell and click the **IP** icon.
14. In the **Value** text box, enter **`10.1.10.11`**.

    10.1.10.11 is the IP address of web-sv-01a virtual machine.

15. Click **OK**.
16. Point to the **Service** cell and click the pencil icon.
17. In the **Filter** box, enter **`http`** and press Enter.
18. In the Available Objects list, select **HTTP** and **HTTPS** and click the right arrow to move them to the Selected Objects list.
19. Click **OK**.
20. Click **Publish Changes**.
21. From the **NSX Manager** drop-down menu, select **172.20.110.43 (Role: Secondary)**.
22. Verify that the Universal Section and the rule in the Universal Section are already replicated to the secondary NSX Manager instance.

Answer Key

Lab 2: Configuring and Deploying an NSX Controller Cluster

Task 3: Verify That the First NSX Controller Instance Is Operational 10

1. Powered on, based on the activated Play icon.
2. Four.
3. 4,096 MB.
4. 28 GB.
5. pg-SA-Management.
6. An IP address assigned from the controller pool created in task 2.
7. Five.
8. Yes.
9. All five roles.
10. Four or five.
11. Seven ports: 443, 2878, 2888, 3888, 6632, 6633, 7777.

Lab 3: Preparing for Virtual Networking

Task 3: Configure VXLAN on the ESXi Hosts 14

1. One.
2. dvs-SA-Datacenter.

Lab 4: Configuring Logical Switch Networks

Task 3: Verify That Logical Switch Port Groups Appear in vSphere 21

1. Yes, the ID follows the SID keyword in the port group name.

Task 4: Migrate Virtual Machines to Logical Switches 22

1. Yes.
2. No.

Task 5: Test Network Connectivity 23

1. No.
2. Yes.
3. Yes, the web-sv-02a virtual machine.
4. No.
5. No.
6. East-west routing was not established between the logical switch networks.

Lab 5: Configuring and Deploying an NSX Distributed Router

Task 3: Verify the Distributed Router Deployment and Configuration 31

1. Datastore is SA-Shared-01-Remote.
2. sa-esxi-02.vclass.local.
3. One.
4. 512 MB.
5. 584 MB.
6. 512 MB.
7. Two.

Task 4: Test Connectivity 32

1. Yes.
2. Yes.
3. Yes.
4. Yes.
5. Yes, the other node on the Web-Tier network and the router interface.
6. No.
7. No.
8. North-south routing is yet to be established.

Lab 6: Deploying an NSX Edge Services Gateway and Configuring Static Routing

Task 3: Verify the NSX Edge Services Gateway Deployment 38

1. SA-Shared-01-Remote, which is the datastore chosen during the perimeter gateway deployment.
2. sa-esxi-02.vclass.local.
3. One.
4. 512 MB.
5. 584 MB.
6. 512 MB.
7. 10.
8. Two.

Lab 7: Configuring and Testing Dynamic Routing on NSX Edge Appliances

Task 8: Troubleshoot Connectivity Between the Logical Switch Networks and the Management Network 49

1. Yes.
2. No, only directly connected subnets must be advertised.
3. Yes, Direct-connected can be learned, which is sufficient.
4. No.
5. No.
6. No. Connected is the only selection. Static routes should be added.

Lab 9: Configuring NSX Edge High Availability

Task 1: Prepare for the Lab. 64

172.20.11.3 is the perimeter gateway IP address.

Task 2: Configure NSX Edge High Availability 65

1. Two.
2. Any of the ESXi hosts in the SA-Management cluster.
3. Any of the ESXi hosts in the SA-Management cluster.
4. No. vSphere DRS is not enabled on the cluster in this lab environment. However, if vSphere DRS were enabled, the NSX Edge instances would be placed on separate hosts for high availability purposes.

Task 3: Examine the High Availability Service Status and Heartbeat 66

1. Unit [0] is active. This node should be the same for all students at this stage.
2. Yes. All peer nodes in the Peer Host list are Up.
3. Yes, both services are running.

Task 4: Force a Failover Condition 67

1. Perimeter Gateway-1 is active. This node should be the same for all students at this stage.
2. No, vshield-edge-#-0 is unreachable.
3. Yes, both services are running.
4. Yes, from Perimeter Gateway-0 to Perimeter Gateway-1.

Task 5: Restore the Failed Node 68

1. Perimeter Gateway-1 is active. This node should be the same for all students at this stage.
2. Yes.
3. Yes, both services are running.
4. No, the failover node remains active, and the restored node assumes standby status.

Task 6: Clean Up for the Next Lab 69

Lab 10: Configuring Layer 2 Bridging

Task 3: Move the Two Web Servers to the Host That Runs the Distributed Logical Router Control VM 73

Task 4: Examine the Network Connectivity Between Web VMs and Resolve the Problem 73

1. No, because web-sv-01a is connected to a logical switch and web-sv-02a is connected to a port group with VLAN ID 10. An L2 bridge is required to establish connectivity between the two web VMs.
2. Yes. The L2 bridge created in the previous steps established L2 connectivity between the two web VMs.

Lab 11: Configuring and Testing NAT on an NSX Edge Services Gateway

Task 2: Verify Untranslated Packet Addressing 79

1. No.

Task 5: Use the Destination NAT to Test Connectivity 81

1. The untranslated IP address of web-sv-01a.
2. No. Regardless of any TCP flag sequencing or handshake condition that might be set, the IP addresses do not match.

Lab 12: Configuring Load Balancing with NSX Edge Gateway

Task 7: Use the Packet Capture Capabilities of NSX Edge to Verify Round-Robin Load Balancing 92

1. NAT.
2. Because the load balancer is operating in nontransparent mode and proxying sessions between itself and the web servers on behalf of the original client.
3. Transparent mode.

Task 8: Examine NAT Rule Changes 94

1. No, the original and translated IP addresses are both VIP IP address.
2. No.
3. To force the traffic into the NAT logic of the NSX Edge services gateway where a member server can be selected and the destination NAT can be performed. Traffic received on the virtual server IP address must undergo a destination NAT after the destination server is selected from the pool, based on the configured load-balancing algorithm. Because server selection is dynamic, the destination NAT rule triggers the destination NAT operation where further logic can be applied.
4. No, a virtual server cannot operate on a pool of destination NAT-defined addresses. Such functionality would require recursive application of the NAT logic to each packet that is received. The system is not designed to accommodate that type of operation. Only one NAT rule can be applied to any packet received.
5. Uplink-Interface.

Task 10: Reposition the Virtual Server and Examine NAT Rule Changes 96

1. Yes.
2. No.
3. No, the operations are the same.
4. The destination NAT occurs on the outbound interface. In this case, that is vNic_2, which faces the network that the member servers are attached to. The previous destination NAT rule was applied on the receiving interface because destination NAT rules must be applied on the interface connected to the network that contains the original IP address to be translated, regardless of ingress or egress.

Lab 14: Configuring Layer 2 VPN Tunnels

Task 10: Test Tunnel Connectivity 116

1. The address of the web-sv-01b virtual machine.
2. The MAC address of web-sv-01b, because the tunnel wraps L2 traffic and, when decapsulated, the hardware address is preserved.
3. Yes.
4. Yes. Tunnel decapsulation ensures the original source MAC/IP address.

Lab 16: Configuring and Testing SSL VPN-Plus

Task 8: Review the Client Configuration, and Examine Traffic 135

1. IP address of the remote gateway:443.
2. Web-Tier subnet 10.2.40.0/255.255.255.0.
3. An IP address from the range configured for the IP pool.
4. The IP address assigned to the SSL VPN-Plus client from the IP pool specified in the tunnel profile.

Lab 17: Using NSX Distributed Firewall Rules to Control Network Traffic

Task 4: Restrict Inbound Web Server Traffic to HTTP and HTTPS 141

1. Distributed firewall rules work on true source and destination addresses and objects. Such rules are not affected by transforms (such as destination NAT) performed by NSX Edge devices.

Lab 18: Using NSX Edge Firewall Rules to Control Network Traffic

Task 3: Determine How the Firewall Rule Interacts with Other NSX Edge Features 151

1. No.

Lab 22: Micro-Segmentation with Application Rule Manager

Task 3: Analyze the Traffic Flow Session Results 175

1. They are consolidated by direction IN and INTRA and by Source and Destination versus individual processed packets.
2. You can define both dynamic memberships and static inclusion and exclusion objects.
3. app-sv-01a, db-sv-01a, web-sv-01a, and web-sv-02a/
4. The objects were specified in the Flow Monitoring session of Application Rule Manager.

Task 4: Publish and Analyze the Application Rule Manager Recommendations 176

1. Yes.

Lab 23: Guest Introspection and Endpoint Monitoring

Task 4: Analyze the Data Collection Results 180

1. Two virtual machines are running: Windows7 and Windows7-2. They are the only Windows-based VMs in the inventory.
2. The number is usually three: iexplorer, lsass, and putty.
3. The Process Flows tab displays the details.
4. Windows7 and Windows7-2.
5. The VM Details window displays the Process Generating Traffic details.
6. Two users are listed: administrator and normalusera.
7. The User Flows Details pop-up window appears.