VMware vCloud Networking and Security for vSphere Professionals

Lab Manual
vCloud Networking and Security 5.5

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

VMware vCloud Networking and Security for vSphere Professionals
vCloud Networking and Security 5.5
Part Number EDU-EN-NS55-LAB
Lab Manual
Revision A

Copyright/Trademark

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.

Course development: Rob Nendel

Technical review: Phil Cohen, Mark Jones

Technical editing: PJ Schemenaur

Production and publishing: Rhonda Jones, Regina Aboud

The courseware for VMware instructor-led training relies on materials developed by the VMware Technical Communications writers who produce the core technical documentation, available at http://www.vmware.com/support/pubs.

www.vmware.com/education

Table of Contents

Lab 1

Installing and Configuring VMware vCloud Networking and Security

Objective: Install and configure vCloud Networking and Security

In this lab, you will perform the following tasks:

1. License vCenter Server and ESXi Hosts
2. Configure vShield Manager Network Settings
3. Configure vShield Manager
4. Apply an SSL Certificate to Identify the vShield Manager Web Service
5. Change the vShield Manager Default Administrator Password
6. Review the vShield Manager Inventory
7. License vCloud Networking and Security

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: License vCenter Server and ESXi Hosts

At the beginning of this course, the VMware® vCenter Server™ and VMware ESXi™ hosts are configured to use expired evaluation licenses.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. In the Firefox window, click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client as the vSphere administrator, using the standard lab password.
4. Assign a vCenter Server license key to the vCenter Server instance.
   a. In the left pane, navigate to **Administration > Licenses**.
   b. In the middle pane, click the **vCenter Server Systems** tab.
   c. With the vCenter Server instance selected, click the **Assign License Key** link.
   d. In the Assign License Key panel, select **Assign a new license key** from the drop-down menu.
   e. In the **License key** text box, type or paste your vCenter license key.
   f. Click **OK**.
5. Assign a VMware vCloud® Suite Enterprise license key to each ESXi host.
   a. In the center pane, click the **Hosts** tab.
   b. Select the first ESXi host in the list.
   c. Press the Shift key and click the last ESXi host in the list to select all three ESXi hosts.
   d. Release the Shift key and click the **Assign License Key** link.
   e. In the Assign License Key panel, select **Assign a new license key** from the drop-down menu.
   f. In the **License key** text box, type or paste your vCloud Suite Enterprise license key.
   g. Click **OK**.
   h. In the hosts list, press Shift and click to select all three ESXi hosts.
   i. Right-click the selected hosts and select **Connect** from the pop-up menu. You can also connect each host individually from the **vCenter > Hosts and Clusters** inventory panel.

Task 2: Configure vShield Manager Network Settings

The VMware® vShield Manager™ server has been preconfigured to allow SSH connections. Typically, configuring the vShield Manager network settings is performed from the local console.

Student B performs this task. Student A verifies the settings.

Use the following information from the class configuration handout:

- vShield Manager default administrator user name __________________________
- vShield Manager default administrator password __________________________
- vShield Manager address __________________________
- vShield Manager subnet mask __________________________
- vShield Manager DNS search list __________________________
- Management network gateway address __________________________
- Primary DNS server address __________________________

1. Minimize the Firefox window.
2. On the lab desktop, double-click the **Putty** shortcut.
3. In the PuTTY window, double-click the **vShield Manager** session profile.
4. When prompted, click **Yes** to confirm the PuTTY security alert.
5. Log in by using the vShield Manager default administrator credentials.
6. At the `manager>` prompt, type **`enable`** and press Enter.
7. When prompted, type the vShield Manager default administrator password and press Enter.
8. At the `manager#` prompt, type **`setup`** and configure the vShield Manager server network parameters.

Option	Action
IP Address (A.B.C.D)	Type the vShield Manager address and press Enter.
Subnet Mask	Type the vShield Manager subnet mask and press Enter.
Default Gateway	Type the Management network gateway address and press Enter.
Primary DNS IP	Type the Primary DNS server address and press Enter.

Option	Action
Secondary DNS IP	Press Enter.
DNS domain search list	Type the vShield Manager DNS search list and press Enter.

9. When prompted to save the new configuration, type **y** and press Enter.
10. When prompted to reboot, type **y** and press Enter.

    PuTTY reports a fatal error when connection to the server is lost.
11. Click **OK** to close the dialog box.
12. Close the PuTTY window.
13. On the Windows task bar, click the Firefox application icon to restore the browser window.
14. Wait a few minutes while the vShield Manager server reboots.

Task 3: Configure vShield Manager

After the network settings have been configured, and the server has rebooted, you can log in to the vShield Manager interface to continue initial setup.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- vShield Manager default administrator user name ________________________
- vShield Manager default administrator password ________________________
- vCenter FQDN ________________________
- vSphere administrator user name ________________________
- Standard lab password ________________________
- NTP server address ________________________
- Syslog server address ________________________
- Syslog server port number ________________________

1. In the Firefox window, open a new browser tab.
2. Click the **vShield Manager** favorite link.
3. If the Web page is unavailable, perform the following actions.
    a. Wait 1 minute.

b. Click the **vShield Manager** favorite link.

c. Repeat steps a and b until the Web page responds.

4. Log in to the vShield Manager interface as the default administrator.

NOTE

In the following steps, use the horizontal scroll bar to locate the Edit button for each item to be configured.

5. Configure the Lookup Service.

   The vSphere SSO Lookup service is hosted on the VMware® vCenter™ system.

   a. Click the **Edit** button and configure the Lookup Service settings.

Option	Action
Configure Lookup Service	Select the check box.
Lookup Service Host	Type the vCenter FQDN.
Port	Keep the default of `7444`.
SSO Administrator Username	Type the vSphere administrator user name.
Password	Type the standard lab password.

   b. Click **OK**.

   c. When prompted, click **Yes** to confirm the security warning.

6. Configure the vCenter association.

   a. Click the **Edit** button and configure the vCenter settings.

Option	Action
vCenter Server	Type the vCenter FQDN.
Administrator Username	Type the vSphere administrator user name.
Password	Type the standard lab password.
Assign vShield Enterprise Administrator role to this user	Leave the check box selected.
Modify plug-in script download location	Leave the check box deselected.

b. Click **OK**.

c. When prompted, click **Yes** to confirm the security warning.

7. Configure the NTP server.

   a. Scroll down to locate the NTP Server section.

   b. Click the **Edit** button and configure the NTP server settings.

Option	Action
NTP Server	Type the NTP server address.

   c. Click **OK**.

8. Configure a syslog server.

9. Scroll down to locate the Syslog Server section.

   a. Click the **Edit** button and configure the Syslog server settings.

Option	Action
Syslog Server	Type the Syslog server address.
Port	Type the Syslog server port number.

   b. Click **OK**.

Task 4: Apply an SSL Certificate to Identify the vShield Manager Web Service

Applying an SSL certificate to the vShield Manager interface requires a certificate authority (CA) certificate and a Web server certificate signed by the CA. For class, a pre-signed certificate is provided.

Student B performs this task. Student A verifies the settings.

Use the following information from the class configuration handout:

- vShield Manager default administrator user name ___________________________
- vShield Manager default administrator password ___________________________

1. On the Configuration tab, click the **SSL Certificate** link.
2. Import the root CA certificate.
    1. In the Import Signed Certificate section, click the **Browse** button.
    2. Select the **`CA.cer`** file and click **Open**.
    3. Select **Root CA** from the Certificate Type drop-down menu.
    4. Click the **Apply** button.

       Applying the certificate will take a few seconds to complete.
3. Import the vShield Manager Web server certificate.
    1. Click the **Browse** button.
    2. Select the **`vShieldManager.cer`** file and click **Open**.
    3. Leave the Certificate Type as CA-Signed X.509 Cert.
    4. Click **Apply**.
4. After importing both certificates, click the **Apply Certificate** button at the top of the page.
5. In the Firefox window, close the vShield Manager tab.
6. Wait 2 minutes while the vShield Manager server is restarted.
7. In the Firefox window, open a new browser tab.
8. Click the vShield Manager favorite link.
9. If the Web page is unavailable, perform the following actions.
    1. Wait 1 minute.
    2. Click the **vShield Manager** favorite link.
    3. Repeat steps a and b until you are prompted with a certificate security warning.
10. Click the **I Understand the Risks** link.
11. Click the **Add Exception** button.
12. Click the **View** button to review the certificate details.
13. After reviewing the certificate details, click the **Close** button.
14. Click the **Confirm Security Exception** button.
15. Log in to the vShield Manager interface as the default administrator.

Task 5: Change the vShield Manager Default Administrator Password

The default administrator password can be customized.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- vShield Manager default administrator password ________________________
- Standard lab password ________________________

1. In the right pane, click the **Change Password** link, in the upper-right corner of the vShield Manager interface, in the red bar.
2. In the Change Password panel, customize the default administrator password.

Option	Action
Old password	Type the vShield Manager default administrator password.
New password	Type the standard lab password.
Retype password	Type the standard lab password.

3. Click **OK**.
4. Click the **Logout** link, located in the upper-right corner of the vShield Manager interface.
5. When prompted, click **OK** to confirm the logout operation.
6. Log in to the vShield Manager interface as the default administrator, using the standard lab password.

Task 6: Review the vShield Manager Inventory

The vShield Manager interface includes an inventory tree in the left pane. The inventory tree shows the vSphere data centers, clusters, hosts, and virtual machines.

Student B performs this task. Student A verifies the settings.

Use the following information from the class configuration handout:

- vSphere administrator user name ________________________
- Standard lab password ________________________

1. In the left panel, expand the **Datacenters** item.
2. Select the **Datacenter-A** item.
3. In the right pane, on the General tab, use the Host Information table to verify the following information:
   - Three ESXi hosts are listed.
   - Two clusters are listed.
   - The esxi-02a.vclass.local host is hosting two user virtual machines.
   - The esxi-01a.vclass.local host and esxi-01b.vclass.local host are hosting a total of three virtual machines.
   - No service virtual machines are deployed to the ESXi hosts.
4. In the left pane, expand the **Datacenter-A** item and expand the **Branch** and **HQ** cluster items.
5. For each of the following inventory items, select the item and review the options available in the right pane.
   - Branch
   - esxi-01a.vclass.local

   The summary information updates a few seconds after a host is selected.
6. In the left pane, navigate to **HQ > HQ Application > Web1 > Network adapter 1**.
7. In the right pane, use the summary view to determine the following.
   - The current host
   - The possible host
   - The network to which Network adapter 1 connects

8. In the Firefox window, click the **vSphere Web Client** tab.
9. In the vSphere Web Client interface, click the **Home** icon.
10. In the left pane, navigate to **vCenter > Hosts and Clusters**.
11. Expand the vCenter inventory tree and compare the hierarchy with the vShield Manager inventory.

Task 7: License vCloud Networking and Security

At the beginning of this course, the vCloud Networking and Security is configured to use expired evaluation licenses.

Student A performs this task. Student B verifies the settings.

1. In the vSphere Web Client, click the **Home** icon.
2. In the left pane, navigate to **Administration > Licenses**.
3. In the middle pane, click the **Solutions** tab.
4. If vCloud Networking and Security is not shown in the solutions list, click the **Refresh** button, located to the left of the logged-in user name at the top of the page.
5. Select but do not open the **vCloud Networking and Security** solution item.
6. Click the **Assign License Key** link.
7. In the Assign License Key panel, perform the following actions.
   a. Click the **VMware vCloud Suite Enterprise** license button.
   b. Click **OK**.
8. At the top of the page, click the **Home** icon.

Lab 2

Managing Users and Backups

Objective: Manage user accounts and database backups

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Manually Back Up vShield Manager Data
3. Schedule vShield Manager Backups
4. Restore a vShield Manager Backup
5. Create and Manage Local Users
6. Test User Role Restrictions
7. Log In as the vSphere Administrator

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing class from the previous lab, skip to the next task.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________
- VMware® vShield Manager™ default administrator user name ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. In the Firefox window, click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the vSphere administrator, using the standard lab password.
4. In the Firefox window, open a new browser tab.
5. Click the **vShield Manager** favorite link.
6. Log in to the vShield Manager interface as the default administrator, using the standard lab password.

Task 2: Manually Back Up vShield Manager Data

The vShield Manager database is backed up manually or by a schedule to an FTP or SFTP server.

Student A performs this task. Student B performs the settings.

Use the following information from the class configuration handout:

- FTP server address ________________________
- FTP server user name ________________________
- FTP server directory ________________________
- Standard lab password ________________________

1. In the vShield Manager interface, in the left pane, select **Settings & Reports**.
2. In the right pane, on the Configuration tab, click the **Backups** link.

3. Configure the backup FTP server settings.

Option	Action
Host Name/IP Address	Type the FTP server address.
User Name	Type the FTP server user name.
Password	Type the standard lab password.
Backup Directory	Type the FTP server directory.
Filename Prefix	Leave blank.
Pass Phrase	Leave blank.
Transfer Protocol	Leave FTP selected.

4. Click the **Backup** button.
5. When prompted, click **OK** and allow the backup operation to complete.

   The FTP server is configured to save backups in a folder on the lab desktop.
6. Minimize the Firefox browser window.
7. On the lab desktop, double-click the **vShield Backups** folder.

   The folder contains two files.
8. Close the vShield Backups folder window.

Task 3: Schedule vShield Manager Backups

The vShield Manager database is backed up manually or by a schedule to an FTP or SFTP server.

Student B performs this task. Student A verifies the settings.

Use the following information from the class configuration handout:

- Standard lab password ________________________

1. Restore the Firefox browser window.
2. Configure the backup FTP server settings.

Option	Action
Host Name/IP Address	Type the FTP server address.
User Name	Type the FTP server user name.
Password	Standard lab password.
Backup Directory	Type the FTP server directory.
Filename Prefix	Leave blank.
Pass Phrase	Leave blank.
Transfer Protocol	Leave FTP selected.

3. Configure the backup schedule settings.

Option	Action
Scheduled Backups	Select **On** from the pull-down menu
Backup Frequency	Select **Hourly** from the pull-down menu
Minute	From the pull-down menu, select a minute that is two (2) to five (5) minutes ahead of the lab computer system time
Exclude System Event Logs	Leave the check box deselected
Exclude Audit Logs	Leave the check box deselected

4. Click the **Save Settings** button.
5. Minimize the Firefox browser window.
6. On the lab desktop, double-click the **vShield Backups** folder icon.
7. Monitor the vShield Backups folder until the scheduled backup is performed.

   Two new files appear in the folder when the next scheduled backup occurs.
8. Close the vShield Backups folder window.
9. Restore the Firefox browser window.
10. Disable scheduled backups by configuring the following settings.

Option	Action
Scheduled Backups	Select **Off** from the drop-down menu.
Password	Type the standard lab password.

11. Click the **Save Settings** button.

Task 4: Restore a vShield Manager Backup

The vShield Manager database can be manually restored from a list of existing backups.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- Standard lab password ___________________________
- vShield Manager default administrator user name ___________________________

1. In the **Password** field, type the standard lab password.
2. Click either the **Refresh Backups** or the **View Backups** button.
   The button title varies depending on your student assignment.
3. Select the check box for the last backup in the list.
4. In the Password field, type the standard lab password.
5. Click the **Restore** button.
6. When prompted, click **OK**.
7. Click the **Logout** link, located in the upper-right corner of the vShield Manager interface, in the red bar.

8. When prompted, click **OK**.
9. Wait 2 minutes for the vShield Manager server to reboot.
10. Click the vShield Manager favorite link.
11. If the Web page is unavailable, perform the following actions.
    a. Wait 1 minute.
    b. Click the **vShield Manager** favorite link.
    c. Repeat steps a and b until you are prompted to log in.
12. Log in to the vShield Manager interface as the default administrator, using the standard lab password.

Task 5: Create and Manage Local Users

Local user accounts are created by using the vShield Manager interface.

Student B performs this task. Student A verifies the settings.

1. In the left pane, select **Settings & Reports**.
2. In the right pane, click the **Users** tab.
3. Create a local security administrator account.
    a. On the Users tab, click the **Add** button.
    b. In the Assign Role panel, configure the following local user.

Option	Action
Email	Leave blank.
Login ID	Type **`secadmin`**.
Full name	Leave blank.
Password	Type **`vmware1!`**
Retype password	Type **`vmware1!`**

    c. Click **Next**.
    d. Under Select Roles, select the **Security Administrator** radio button.
    e. Click **Next**.

f. Under Limit Scope, leave the **No restriction** radio button selected.

g. Click **Finish**.

4. Create a local auditor account.

   a. On the Users tab, click the **Add** button.

   b. In the Assign Role panel, configure the following local user.

Option	Action
Email	Leave blank.
Login ID	Type **`auditor`**.
Full name	Leave blank.
Password	Type **`vmware1!`**
Retype password	Type **`vmware1!`**

   c. Click **Next**.

   d. Under Select Roles, leave the **Auditor** radio button selected.

   e. Click **Next**.

   f. Under Limit Scope, leave the **No restriction** radio button selected.

   g. Click **Finish**.

Task 6: Test User Role Restrictions

The actions that a user can perform are controlled by the role assigned to the user. Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- vShield Manager default administrator user name ________________________
- Standard lab password ________________________

1. Click the **Logout** link, located in the upper-right corner of the vShield Manager interface, in the red bar.
2. When prompted, click **OK**.
3. Log in as the local auditor user and examine restrictions.
   a. Log in to the vShield Manager interface as the auditor user with the `vmware1!` password.
   b. In the left pane, select the **Settings & Reports** link.
   c. In the right pane, examine the tabs available to the auditor user.

      The auditor user has access to three tabs, none of which are configuration related.
   d. In the left pane, expand **Datacenters**, and select **Datacenter-A**.
   e. In the right pane, on the **General** tab, click the **Grouping** link.

      All Grouping action icons are disabled.
   f. Click the **Logout** link, located at the upper-right corner of the page.
   g. When prompted, click **OK**.
4. Log in as the local security administrator user and examine restrictions.
   a. Log in to the vShield Manager interface as the secadmin user with the `vmware1!` password.
   b. In the left pane, expand **Datacenters** and select **Datacenter-A**.
   c. In the right pane, on the **General** tab, click the **Grouping** link.

      The Add (green plus symbol) icon is enabled.
   d. Click the **Logout** link, located in the upper-right corner of the page.
   e. When prompted, click **OK**.
5. Log in to the vShield Manager interface as the default administrator, using the standard lab password.

Task 7: Log In as the vSphere Administrator

In addition to local users, vSphere single sign-on users can be imported and assigned vShield Manager roles. When vShield Manager is paired with a VMware® vCenter Server™ instance, the vCenter administrator user is automatically added.

Student B performs this task. Student A verifies the settings.

Use the following information from the class configuration handout:

- vSphere administrator user name ____________________________
- Standard lab password ____________________________

1. In the left pane, select **Settings & Reports.**
2. In the right pane, click the **Users** tab.
3. In the users list, locate the vSphere administrator user.

   The vSphere administrator user is administrator@vsphere.local in this lab.
4. Click the **Logout** link located in the upper-right corner of the page.
5. When prompted, click **OK**.
6. Log in to the vShield Manager interface as the vSphere administrator, using the standard lab password.

Lab 3

Preparing VXLAN Networking

Objective: Configure vSphere and vCloud Networking and Security for VXLAN networking

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Create a Distributed Switch for the HQ Cluster
3. Create a Distributed Switch for the Branch Cluster
4. Prepare VXLAN Connectivity
5. Examine vSphere Networking Changes

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing the class from the previous lab, skip to the next task.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the vSphere administrator, using the standard lab password.
4. In the Firefox window, open a new browser tab.
5. Click the **vShield Manager** favorite link.
6. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.

Task 2: Create a Distributed Switch for the HQ Cluster

A distributed switch or other VXLAN-capable switch component must be configured in vSphere before preparing VMware vCloud® Networking and Security™ virtual networking.

Student A performs this task. Student B verifies the settings.

1. In the Firefox window, click the **vSphere Web Client** tab.
2. In the left pane, navigate to **vCenter > Networking**.
3. Expand the inventory tree and select **Datacenter-A**.
4. Create a 5.5.0 distributed switch for the HQ cluster.
   a. In the middle pane, select **New Distributed Switch** from the **Actions** drop-down menu.
   b. In the New Distributed Switch panel, type **`dvs-HQ-Production`** in the **Name** text box.
   c. Click **Next**.
   d. Under **Select version**, leave the **Distributed switch: 5.5.0** button selected and click **Next**.
   e. Under Edit settings, configure the following distributed switch parameters.

Option	Action
Number of uplinks	Type **2.**
Network I/O Control	Select **Disabled** from the drop-down menu.
Default port group	Deselect the check box.

f. Click **Next**.

g. Under Ready to Complete, click **Finish**.

5. In the inventory tree, select **dvs-HQ-Production**.
6. In the middle pane, select **Add and Manage Hosts** from the **Actions** drop-down menu.
7. In the Add and Manage Hosts panel, leave the **Add hosts** radio button selected and click **Next**.
8. Under Select hosts, click the **New Hosts** link.
9. In the Select new hosts panel, select the **esxi-01a.vclass.local** and **esxi-01b.vclass.local** check boxes and click **OK**.
10. Click **Next**.
11. Under Select network adapter tasks, deselect the **Manage VMkernel adapters** check box.
12. Click **Next**.
13. Under Manage physical network adapters, perform the following actions for the esxi-01a.vclass.local host.
    a. Select **vmnic3** and click **Assign uplink**.
    b. In the Select an Uplink for vmnic3 dialog box, leave **Uplink 1** selected and click **OK**.
    c. Select **vmnic4** and click **Assign uplink**.
    d. In the Select an Uplink for vmnic4 dialog box, leave **Uplink 2** selected and click **OK**.
14. Perform the following actions for the esxi-01b.vclass.local host.
    a. Select **vmnic3** and click **Assign uplink**.
    b. In the Select an Uplink for vmnic3 dialog box, leave **Uplink 1** selected and click **OK**.
    c. Select **vmnic4** and click **Assign uplink**.
    d. In the Select an Uplink for vmnic4 dialog box, leave **Uplink 2** selected and click **OK**.
15. Click **Next**.
16. Under **Analyze impact**, click **Next**.

17. Under **Ready to Complete**, click **Finish**.

18. Verify that the distributed switch uplink connections are configured correctly.

    a. In the center pane, click the **Manage** tab.

    b. With the Topology link selected, use the horizontal scroll bars to view the dvs-HQ-Production uplink connections.

    c. Expand **Uplink 1** and verify that the esxi-01a.vclass.local and esxi-01b.vclass.local hosts are connected.

    d. Expand **Uplink 2** and verify that the esxi-01a.vclass.local and esxi-01b.vclass.local hosts are connected.

Task 3: Create a Distributed Switch for the Branch Cluster

A distributed switch or other VXLAN-capable switch component must be configured in vSphere before preparing vCloud Networking and Security virtual networking.

Student B performs this task. Student A verifies the settings.

1. Create a 5.5.0 distributed switch for the Branch cluster.

    a. In the left pane, select **Datacenter-A**.

    b. In the middle pane, select **New Distributed Switch** from the **Actions** drop-down menu.

    c. In the New Distributed Switch panel, type **`dvs-Branch-Production`** in the **Name** text box.

    d. Click **Next**.

    e. Under Select version, leave the **Distributed switch 5.5.0** button selected and click **Next**.

    f. Under Edit settings, configure the following distributed switch parameters.

Option	Action
Number of uplinks	Type **2.**
Network I/O Control	Select **Disabled** from the drop-down menu.
Default port group	Deselect the check box.

    g. Click **Next**.

    h. Under Ready to Complete, click **Finish**.

2. In the left pane, select **dvs-Branch-Production**.

3. In the center pane, select **Add and Manage Hosts** from the **Actions** drop-down menu.
4. In the Add and Manage Hosts panel, leave the **Add hosts** radio button selected, and click **Next**.
5. Under Select hosts, click the **New Hosts** link.
6. In the Select new hosts panel, select the **esxi-02a.vclass.local** check box and click **OK**.
7. Click **Next**.
8. Under Select network adapter tasks, deselect the **Manage VMkernel adapters** check box.
9. Click **Next**.
10. Under Manage physical network adapters, perform the following actions.
    a. Select **vmnic3** and click **Assign uplink**.
    b. In the Select an Uplink for vmnic3 dialog box, leave **Uplink 1** selected and click **OK**.
    c. Select **vmnic4** and click **Assign uplink**.
    d. In the Select an Uplink for vmnic4 dialog box, leave **Uplink 2** selected and click **OK**.
11. Click **Next**.
12. Under Analyze impact, click **Next**.
13. Under Ready to Complete, click **Finish**.
14. Verify that the distributed switch uplink connections are configured correctly.
    a. In the center pane, click the **Manage** tab.
    b. With the Topology link selected, use the horizontal scroll bars to view the dvs-Branch-Production uplink connections.
    c. Expand **Uplink 1** and verify that esxi-02a.vclass.local host is connected.
    d. Expand **Uplink 2** and verify that esxi-02a.vclass.local host is connected.

Task 4: Prepare VXLAN Connectivity

In most situations, the network administrator provides the multicast range for VXLAN operations. A multicast address is required for each VXLAN to be created.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- HQ network _________________________
- Branch network _________________________

1. In the Firefox window, click the **vShield Manager** tab.
2. In the left pane, expand the **Datacenters** container and select the **Datacenter-A** item.
3. In the right pane, click the **Network Virtualization** tab.
4. Click the **Preparation** link.
5. Configure the Segment ID parameters.
   a. Click the **Segment ID** button.
   b. Click the **Edit** button located on the far right of the vShield Manager interface.
   c. In the Edit Settings panel, configure the following VXLAN parameters.

Option	Action
Segment ID pool	Type **`5000-5255`**.
Multicast addresses	Type **`225.1.1.0-225.1.1.255`**.

   d. Click **OK**.
6. Configure cluster connectivity.
   a. Click the **Connectivity** button.
   b. Click the **Edit** button located on the far right of the vShield Manager interface.
   c. Prepare the Branch cluster by configuring the following settings.

Option	Action
Use	Select the check box.
Distributed Switch	Select **dvs-Branch-Production** from the drop-down menu.
VLAN	Leave the default of zero.

d. Prepare the HQ cluster by configuring the following settings.

Option	Action
Use	Select the check box.
Distributed Switch	Select **dvs-HQ-Production** from the drop-down menu.
VLAN	Leave the default of zero.

e. Click **Next**.

f. Under Specify transport attributes, select **Fail Over** from the Teaming Policy drop-down menu, for each distributed switch.

g. Leave the MTU (bytes) value at `1600` for each distributed switch.

h. Click **Finish**.

7. Verify cluster and host readiness.

a. When the status of both clusters is `Ready`, expand the **HQ** and **Branch** items.

b. Verify the following:

- The status of each ESXi host is `Ready`.
- Each vmnic has acquired an appropriate DHCP-assigned address.

esxi-01a.vclass.local has an IP address in the HQ network range.

esxi-01b.vclass.local has an IP address in the HQ network range.

esxi-02a.vclass.local has an IP address in the Branch network range.

Task 5: Examine vSphere Networking Changes

Changes made to vSphere by vCloud Networking and Security can be reviewed by using the vSphere Web Client.

Student B performs this task. Student A verifies the settings.

1. In the Firefox window, click the **vSphere Web Client** tab.
2. In the left pane, expand the **dvs-HQ-Production** and **dvs-Branch-Production** distributed switch items.
3. Verify that a new port group has been added to each distributed switch.

The port group name starts with vxw-vmknicPg-dvs-.

4. In the left pane, click the **Hosts and Clusters** icon.
5. Under HQ, select the **esxi-01a.vclass.local** host item.
6. In the middle pane, click the **Manage** tab.
7. On the Manage tab, click the **Networking** button.
8. Select the **Virtual adapters** category.
9. In the Virtual adapters list, select the **vmk3** adapter and use the horizontal scroll bar to examine the adapter details.
10. In the left pane, select **HQ > esxi-01b.vclass.local**.
11. In the center pane, examine the **vmk3** adapter details.
12. In the left pane, select **Branch > esxi-02a.vclass.local**.
13. In the center pane, examine the **vmk3** adapter details.
14. In the Firefox window, click the **vShield Manager** tab.

Lab 4

Configuring VXLAN Networking

Objective: Configure VXLAN networking in vCloud Networking and Security

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Create Network Scopes
3. Create VXLAN Virtual Wires
4. Connect Virtual Machines to the HQ Network Virtual Wire
5. Connect Virtual Machines to the Shared Network Virtual Wire
6. Connect Virtual Machines to the Branch Network Virtual Wire
7. Examine vSphere Networking Changes

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing the class from the previous lab, skip to the next task.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the vSphere administrator, using the standard lab password.
4. In the left pane, navigate to **vCenter > Networking**.
5. Expand the vCenter inventory.
6. In the Firefox window, open a new browser tab.
7. Click the **vShield Manager** favorite link.
8. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.
9. In the left pane, expand the **Datacenters** container and select **Datacenter-A**.
10. In the right pane, click the **Network Virtualization** tab.

Task 2: Create Network Scopes

The lab environment consists of three different network scopes, one scope for each cluster and one scope that spans both clusters.

Student A performs this task. Student B verifies the settings.

1. In the vShield Manager interface, on the Network Virtualization tab, select the **Network Scopes** link.
2. Create a network scope that spans both clusters.
    a. Click the **Add** (green plus symbol) icon.

b. In the Add Network Scope panel, configure the Shared Scope settings.

Option	Action
Name	Type **`Shared Scope`**.
Branch	Select the check box.
HQ	Select the check box.

c. Click **OK**.

d. In the network scopes list, click the **Shared Scope** link.

e. In the Summary view, verify the following configuration values.

- Total Networks is `0`.
- The HQ and Branch clusters are present with a VXLAN Transport Status of `Ready`.
- The PortProfile is present and available.

f. Click the blue **back-arrow** icon.

3. Create a network scope that includes only the HQ cluster.

a. Click the **Add** (green plus symbol) icon.

b. In the Add Network Scope panel, configure the HQ Scope settings.

Option	Action
Name	Type **`HQ Scope`**.
Branch	Leave the check box deselected.
HQ	Select the check box.

c. Click **OK**.

d. In the network scopes list, click the **HQ Scope** link.

e. In the Summary view, verify the following configuration values.

   - Total Networks is `0`.
   - The HQ cluster is present with a VXLAN Transport Status of Ready.
   - The Branch cluster is not present.
   - The PortProfile is present and available.

f. Click the blue **back-arrow** icon.

4. Create a network scope that includes only the Branch cluster.

a. Click the **Add** (green plus symbol) icon.

b. In the Add Network Scope panel, configure the Branch Scope settings.

Option	Action
Name	Type **`Branch Scope`**.
Branch	Select the check box.
HQ	Leave the check box deselected.

c. Click **OK**.

d. In the network scopes list, click the **Branch Scope** link.

e. In the Summary view, verify the following configuration values.

   - Total Networks is `0`.
   - The Branch cluster is present with a VXLAN Transport Status of Ready.
   - The HQ cluster is not present.
   - The PortProfile is present and available.

f. Click the blue **back-arrow** icon.

Task 3: Create VXLAN Virtual Wires

After network scopes have been created, VXLAN virtual wires can be configured. Each VXLAN virtual wire represents a separate network that is limited by the associated network scope.

Student B performs this task. Student A verifies the settings.

1. On the Network Virtualization tab, click the **Networks** link.
2. Create a VXLAN virtual wire that spans both clusters.
   a. Click the **Add** (green plus symbol) icon.
   b. In the Create VXLAN Network panel, configure the Shared Network settings.

Option	Action
Name	Type **`Shared Network`**.
Network Scope	Select **Shared Scope** from the drop-down menu.

   c. Click **OK**.
   d. In the networks list, verify the following configuration values for the Shared Network item.
      - The Status is `OK`.
      - The Segment ID is `5000`.
      - The Multicast IP Address is `225.1.1.0`.
3. Create a VXLAN virtual wire that is limited to the HQ cluster.
   a. Click the **Add** (green plus symbol) icon.
   b. In the Create VXLAN Network panel, configure the HQ Network settings.

Option	Action
Name	Type **`HQ Network`**.
Network Scope	Select **HQ Scope** from the drop-down menu.

   c. Click **OK**.

d. In the networks list, verify the following configuration values for the HQ Network item.

  - The Status is `OK`.
  - The Segment ID is `5001`.
  - The Multicast IP Address is `225.1.1.1`.

4. Create a VXLAN virtual wire that is limited to the Branch cluster.

   a. Click the **Add** (green plus symbol) icon.

   b. In the Create VXLAN Network panel, configure the Branch Network settings.

Option	Action
Name	Type **`Branch Network`**.
Network Scope	Select **Branch Scope** from the drop-down menu.

   c. Click **OK**.

   d. In the networks list, verify the following configuration values for the Branch Network item.

  - The Status is `OK`.
  - The Segment ID is `5002`.
  - The Multicast IP Address is `225.1.1.2`.

Task 4: Connect Virtual Machines to the HQ Network Virtual Wire

A virtual machine connection to the HQ Network virtual wire is configured in the vShield Manager interface.

Student A performs this task. Student B verifies the settings.

1. In the networks list, click the **HQ Network** link.
2. Click the **Virtual Machines** button.
3. Click the **Connect** (green plus symbol) icon.
4. In the Connect VNics to this Network panel, click the **Search** (magnifying glass) icon.
5. Select the **Web1** and **Web2** virtual NIC check boxes and click **Next**.
6. Click **Finish** and wait for the virtual machines to appear in the list.

7. For the Web1 virtual machine, verify the following configuration values.
   - The host is esxi-01a.vclass.local or esxi-01b.vclass.local.
   - The state is Powered Off.
   - The virtual NIC count is 1.
   - The total virtual NIC count is 1.
8. For the Web2 virtual machine, verify the following configuration values.
   - The host is esxi-01a.vclass.local or esxi-01b.vclass.local.
   - The state is Powered Off.
   - The virtual NIC count is 1.
   - The total virtual NIC count is 1.
9. Click the **Refresh** link, located near the upper-right corner of the page, under the Network Virtualization tab.

Task 5: Connect Virtual Machines to the Shared Network Virtual Wire

A virtual machine connection to the Shared Network virtual wire is configured in the vShield Manager interface.

Student B performs this task. Student A verifies the settings.

1. In the networks list, click the **Shared Network** item link.
2. Click the **Virtual Machines** button.
3. Click the **Connect** (green plus symbol) icon.
4. In the Connect VNics to this Network panel, click the **Search** (magnifying glass) icon.
5. Select the **Web3** and **Web4** virtual NIC check boxes and click **Next**.
6. Click **Finish** and wait for the virtual machines to appear in the list.
7. For the Web3 virtual machine, verify the following configuration values.
   - The host is esxi-01a.vclass.local or esxi-01b.vclass.local.
   - The state is Powered Off.
   - The virtual NIC count is 1.
   - The total virtual NIC count is 1.

8. For the Web4 virtual machine, verify the following configuration values.
   - The host is esxi-02a.vclass.local.
   - The state is Powered Off.
   - The virtual NIC count is 1.
   - The total virtual NIC count is 1.
9. Click the **Refresh** link, located near the upper-right corner of the page, under the Network Virtualization tab.

Task 6: Connect Virtual Machines to the Branch Network Virtual Wire

A virtual machine connection to the Branch Network virtual wire is configured in the vShield Manager interface.

Student A performs this task. Student B verifies the settings.

1. In the networks list, click the **Branch Network** item link.
2. Click the **Virtual Machines** button.
3. Click the **Connect** (green plus symbol) icon.
4. In the Connect VNics to this Network panel, click the **Search** (magnifying glass) icon.
5. Select the **Web5** virtual NIC check box and click **Next**.
6. Click **Finish** and wait for the virtual machine to appear in the list.
7. For the Web5 virtual machine, verify the following configuration values.
   - The host is esxi-02a.vclass.local.
   - The state is Powered Off.
   - The virtual NIC count is 1.
   - The total virtual NIC count is 1.
8. Click the **Refresh** link, located near the upper-right corner of the page, under the Network Virtualization tab.

Task 7: Examine vSphere Networking Changes

You use the vSphere Web Client to review changes made to vSphere by VMware vCloud® Networking and Security™.

Student B performs this task. Student A verifies the settings.

1. In the Firefox window, click the **vSphere Web Client** tab.
2. In the left pane, click the **Networking** icon.
3. At the top of the page, click the **Refresh** icon, located to the left of the logged-in user name.
4. In the left pane, examine the dvs-Branch-Production distributed switch port groups.

   Two additional port groups have been added to the distributed switch. Each port group represents a VXLAN virtual wire network.
5. Select either of the new dvs-Branch-Production port groups.

   The new port groups have a name starting with `vxw-dvs-##`.
6. In the center pane, click the **Summary** tab.
7. At the top of the Summary view, find the full name of the port group and verify the following.
   - The sid value is in the range of 5000–5255.
   - The port group name ends with the name of a VXLAN virtual wire.
8. In the Firefox window, click the **vShield Manager** tab.

Lab 5

Testing VXLAN Network Connectivity

Objective: Test virtual networking at the cluster, network, and virtual wire levels

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Verify ESXi Host VXLAN Participation
3. Test Connectivity at the Cluster Level
4. Test Connectivity at the Virtual Network Level
5. Test Connectivity at the Virtual Wire Level

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing class from the previous lab, skip to the next task.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the vSphere administrator, using the standard lab password.
4. In the vSphere Web Client, navigate to **vCenter > Networking**.
5. In the Firefox window, open a new browser tab.
6. Click the **vShield Manager** favorite link.
7. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.
8. In the left pane, expand the **Datacenters** container and select **Datacenter-A**.
9. In the right pane, click the **Network Virtualization** tab.

Task 2: Verify ESXi Host VXLAN Participation

VMware ESXi™ host participation in VXLAN networking can be determined by using the `esxcli` command.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- ESXi root user name ________________________
- Standard lab password ________________________

1. Minimize the Firefox window.
2. On the lab desktop, double-click the **Putty** shortcut.
3. In the PuTTY window, double-click the **ESXi - 01A (HQ)** session.
4. When prompted, click **Yes** to acknowledge the PuTTY security alert.
5. Log in as the ESXi root user, using the standard lab password.

6. At the shell prompt, type the following command and press Enter.

   ```
   esxcli network vswitch dvs vmware vxlan list
   ```

7. Use the command output to verify the following configuration values.
   - The `dvs-HQ-Production` or `dvs-Branch-Production` distributed switch is listed.
   - The MTU is `1600`.
   - The Network count is `0`.
   - The Vmknic Count is `1`.
8. Close the PuTTY window.
9. When prompted, click **OK**.
10. For each of the following hosts, start PuTTY and repeat steps 4 through 8.

Host	PuTTY Session
esxi-01b.vclass.local	ESXi - 01B (HQ)
esxi-02a.vclass.local	ESXi - 02A (Branch)

11. Restore the Firefox window.

Task 3: Test Connectivity at the Cluster Level

You can test VXLAN connectivity at the cluster level.

Student B performs this task. Student A verifies the settings.

1. In the vShield Manager interface, on the Network Virtualization tab, click the **Network Scopes** link.
2. In the network scopes list, click the **Shared Scope** link.
3. Click the **Clusters** button.
4. Click the **Gear** icon, and select **Test Connectivity**.
5. In the Broadcast Test in a Network Scope panel, click the **Browse** button.
6. Select the **esxi-01a.vclass.local** radio button and click the **Select** button.
7. Leave the Size of the test packet as **VXLAN Standard**.
8. Click the **Start Test** button and wait for the test to run to completion.

9. Examine the test results and verify the following conditions.
    - Three hosts responded.
    - One host did not respond.
    - The unresponsive host is the esxi-02a.vclass.local host.

    NOTE

    The unresponsive host condition is expected. The VXLAN tests available in the vShield Manager interface do not test VXLAN transport across a routed network topology. In the lab environment, separate transport networks are used for the HQ and Branch clusters, with a router providing connectivity.

10. Close the Broadcast Test in a Network Scope panel.

Task 4: Test Connectivity at the Virtual Network Level

VXLAN connectivity can be tested at the network level.

Student A performs this task. Student B verifies the settings.

1. On the Network Virtualization tab, click the **Networks** link.
1. In the networks list, click the **Shared Network** item link.
2. Click the **Hosts** button.
3. Click the **Gear** icon and select **Test Connectivity**.
4. Click the Source host **Browse** button and select the **esxi-01a.vclass.local** radio button.
5. Click the **Select** button.
6. Click the Destination host **Browse** button and select the **esxi-01b.vclass.local** radio button.
7. Click the **Select** button.
8. Leave the Size of test packet as **VXLAN Standard**.
9. Click the **Start Test** button and allow the test to run to completion.
10. When the test is complete, verify that three packets were transmitted from the esxi-01a.vlcass.local host and that three packets were received by the esxi-01b.vclass.local host.
11. Click the Destination host **Browse** button and select the **esxi-02a.vclass.local** radio button.
12. Click the **Select** button.
13. Leave the Size of test packet as **VXLAN Standard**.
14. Click the **Start Test** button and wait for the test to run to completion.

15. When the test is complete, verify that the test failed and displayed a Network Is Unreachable error message.

    NOTE

    The test failure is expected because the HQ cluster transport network is separated from the Branch cluster transport network by a router. VXLAN networking across a routed topology uses a route-learning mechanism that is not used during tests.

16. Close the Test Connectivity Between Hosts in the Network panel.
17. Click the blue **back-arrow** button.

Task 5: Test Connectivity at the Virtual Wire Level

To properly test layer-2 connectivity, power on virtual machines connected to the same virtual wire network.

Student A and student B perform this task. Student A powers on the virtual machines.

Use the following information from the class configuration handout:

- Client administrator user name ________________________
- Standard lab password ________________________

1. In the Firefox window, click the **vSphere Web Client** tab.
2. In the left pane, click the **Hosts and Clusters** icon.
3. Power on the Shared Network virtual machines by performing the following actions.
    a. In the left pane, select the **HQ** > **HQ Application** > **Web3** virtual machine item.
    b. In the center pane, select **Power On** from the **Actions** drop-down menu.
    c. In the left pane, select the **Branch** > **Branch Application** > **Web4** virtual machine item.
    d. In the center pane, select **Power On** from the **Actions** drop-down menu.
4. Open a console to the Web3 and Web4 virtual machines by performing the following steps.
    a. In the left pane, select **HQ** > **HQ Application** > **Web3**.
    b. In the center pane, select **Open Console** from the **Actions** drop-down menu.
    c. In the Firefox window, click the **vSphere Web Client** tab.
    d. In the left pane, select **Branch** > **Branch Application** > **Web4**.
    e. In the center pane, select **Open Console** from the **Actions** drop-down menu.

5. In the Firefox window, on the Web4 tab, wait for the virtual machine to power on.
6. Click the **Send Ctrl-Alt-Delete** button in the upper-left corner of the page.
7. Log in to the virtual machine as the client administrator, using the standard lab password.
8. On the Web4 desktop, double-click the **Command Prompt** shortcut.
9. In the Command Prompt window, type the following command to examine the client IP configuration.

   ```
   ipconfig
   ```
10. Verify the following IP configuration values.
    a. The client has not been configured with a default gateway.
    b. The client IP address is `192.168.1.200`.
11. Close the Command Prompt window.
12. In the Firefox window, click the **Web3** tab.
13. Click the **Send Ctrl-Alt-Delete** button, located in the upper-left corner of the page.
14. Log in to the virtual machine as the client administrator, using the standard lab password.
15. On the Web3 desktop, double-click the **Command Prompt** shortcut.
16. In the Command Prompt window, type the following command to examine the client IP configuration.

    ```
    ipconfig
    ```
17. Verify the following IP configuration values.
    a. The client has not been configured with a default gateway.
    b. The client IP address is `192.168.1.100`.
18. To flush the ARP table, execute the following commands.

    ```
    arp -d
    arp -a
    ```
19. Test connectivity between the Web3 and Web4 virtual machines by typing the following command.

    ```
    ping 192.168.1.200
    ```

    NOTE

    The ping operation generates replies from the `192.168.1.200` client machine.

20. Examine the client ARP table again by typing the following command.

    ```
    arp -a
    ```

21. Verify that the `192.168.1.200` virtual machine is listed in the ARP table with a valid physical address in the form of `00-50-56-xx-xx-xx`.

22. Close the Command Prompt window.

23. In the Firefox window, close the Web3 and Web4 tabs.

24. Examine the network diagram handout and verify that the Web3 and Web4 virtual machines have no direct connectivity across the routed topology.

Lab 6

Deploying a VMware vShield Edge Appliance

Objective: Create and deploy a vShield Edge appliance to establish external connectivity and basic services for a VXLAN virtual wire

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Create a Port Group for External Access
3. Create a vShield Edge Appliance for the Shared Network Virtual Wire
4. Configure a Syslog Server
5. Deploy a vShield Edge Appliance to the HQ Cluster
6. Add an Internal Interface for the Shared Network Virtual Wire
7. Configure Basic Edge Services
8. Examine Changes in vSphere
9. Test Basic Services and Verify External Network Connectivity

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing class from the previous lab, skip to the next task.

Student B performs this task. Student A verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the vSphere administrator, using the standard lab password.
4. In the vSphere Web Client interface, navigate to **vCenter > Hosts and Clusters**.
5. Power on the following virtual machines.
   - Branch > Branch Application > Web4
   - HQ > HQ Application > Web3
6. In the Firefox window, open a new browser tab.
7. Click the **vShield Manager** favorite link.
8. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.
9. In the left pane, expand the **Datacenters** container and select **Datacenter-A**.
10. In the right pane, click the **Network Virtualization** tab.

Task 2: Create a Port Group for External Access

A port group that has not been allocated for VXLAN virtual wires must be available to provide external network access to each VMware® vShield Edge™ uplink interface.

Student B performs this task. Student A verifies the settings.

1. In the Firefox window, click the **vSphere Web Client** tab.
2. In the left pane, click the **Networking** icon.
3. Select the **dvs-HQ-Production** distributed switch item.
4. In the center pane, select **New Distributed Port Group** from the **Actions** drop-down menu.

5. In the New Distributed Port Group panel, type **`pg-HQ-External`** in the **Name** text box.
6. Click **Next**.
7. Under Configure settings, click **Next** to accept all default configuration values.
8. Under Ready to Complete, click **Finish**.

Task 3: Create a vShield Edge Appliance for the Shared Network Virtual Wire

A vShield Edge appliance is first defined as an appliance configuration that includes up to 10 network interfaces.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- vSphere administrator user name ________________________
- Standard lab password ________________________
- HQ network gateway address ________________________

1. In the Firefox window, click the **vShield Manager** tab.
2. In the right pane, on the Network Virtualization tab, click the **Edges** link.
3. Click the **Add** (green plus symbol) icon.
4. In the Add Edge panel, provide the following HQ-Edge settings.

Option	Action
Name	Type **`HQ-Edge.`**
Hostname	Leave blank.
Description	Leave blank.
Tenant	Leave blank.
Enable HQ	Leave deselected.

5. Click **Next**.

6. Under CLI Credentials, provide the following SSH access settings.

Option	Action
User Name	Keep the default of `admin`.
Password	Type the standard lab password.
Enable SSH access	Select the check box.

7. Click **Next**.
8. Under Edge Appliances, click **Next**.

   You deploy an appliance in another task.
9. Under Interfaces, click the **Add** (green plus symbol) icon.
10. In the Add Edge Interface panel, perform the following actions.
    a. Type **`External`** in the **Name** text box.
    b. For Type, leave the **Uplink** radio button selected.
    c. Click the **Connected To** drop-down menu and select **pg-HQ-External**.
    d. For Connectivity Status, leave the **Connected** radio button selected.
    e. Under Configure Subnets, click the **Add** (green plus symbol) icon.
    f. In the Add Subnet panel, click the **Add** (green plus symbol) icon to configure the IP address and subnet for the HQ-Edge external interface.

Option	Action
IP Address	Type **`172.20.11.11`** in the text box and click **OK**.
Subnet Mask	Type **`255.255.255.0`** in the text box and click **Save**.

    g. Use the vertical scroll bar to find the MTU setting and verify that the MTU is set to `1500`.
    h. Click the **Add** button.
11. Click **Next**.

12. Under Default Gateway, configure the next hop settings for the HQ-Edge external interface.

Option	Action
Configure Default Gateway	Select the check box.
vNIC	Leave **External** selected.
Gateway IP	Type the HQ network gateway address in the text box.
MTU	Verify that the MTU is `1500`.

13. Click **Next**.
14. Under Firewall & HA, provide the following default policy settings.

Option	Action
Configure Firewall default policy	Select the check box.
Default Traffic Policy	Select the **Accept** radio button.
Logging	Select the **Enable** radio button.

15. Click **Next**.
16. Under Summary, click **Finish**.

Task 4: Configure a Syslog Server

A syslog server can be configured for each vShield Edge appliance.

Student B performs this task. Student A verifies the settings.

Use the following information from the class configuration handout:

- Syslog server address ________________________

1. In the vShield Edge list, select the **HQ-Edge** instance.
2. Click the **Actions** drop-down menu and select **Manage**.
3. In the HQ-Edge > Settings view, find the **Details** section.
4. In the Details section, click the **Change** link.

5. In the Edit Syslog Servers Configuration panel, configure the syslog server to be used by all instances of HQ-Edge.

Option	Action
Syslog Server 1	Type the syslog server address in the text box.
Syslog Server 2	Leave blank.
Protocol	Leave the default of **tcp** selected.

6. Click **Save**.

Task 5: Deploy a vShield Edge Appliance to the HQ Cluster

When deploying a vShield Edge appliance, you must specify the hosting cluster and the datastore. Cluster selection limits by which VXLAN virtual wires can be attached to the appliance.

Student A performs this task. Student B verifies the settings.

1. Use the vertical scroll bar to find the **Edge Appliances** section at the bottom of the HQ-Edge > Settings page.
2. Click the **Add** (green plus symbol) icon.
3. In the Add Edge Appliance panel, select the cluster and datastore to host the HQ-Edge appliance.

Option	Action
Cluster/Resource Pool	Select **HQ Infrastructure** from the drop-down menu.
Datastore	Select **Shared-Datastore** from the drop-down menu.

4. Click **Add**.
5. Use the vertical scroll bar to move to the top of the page.
6. Monitor the current job status to completion.

   The current job status is displayed under the row of buttons, at the top of the page. When the deployment job completes, the current job status disappears.

Task 6: Add an Internal Interface for the Shared Network Virtual Wire

VXLAN virtual wires can be attached to available vShield Edge appliance network interfaces.

Student B performs this task. Student A verifies the settings.

1. Click the **HQ-Edge > Configure** button.
2. In the list, select the **vnic1** interface item.
3. Click the **Edit** (pencil) icon.
4. In the Edit Edge Interface panel, perform the following actions.

   a. Type **`Shared Network`** in the **Name** text box.

   b. For Type, leave the **Internal** radio button selected.

   c. Click the **Select** link, located right of the **Connected To** text box.

   d. In the Connect Edge to a Network panel, select the **Shared Network** radio button and click **Select**.

   e. For Connectivity Status, leave the **Connected** radio button selected.

   f. Under Configure Subnets, click the **Add** (green plus symbol) icon.

   g. In the Add Subnet panel, click the **Add** (green plus symbol) icon to configure the IP address and subnet of the HQ-Edge interface that connects to the Shared Network virtual wire.

Option	Action
IP Address	Type **`192.168.1.1`** in the text box and click **OK**.
Subnet Mask	Type **`255.255.255.0`** in the text box and click **Save**.

   h. Use the vertical scroll bar to find the MTU setting and verify that the MTU is set to `1500`.

   i. Click **Save**.

Task 7: Configure Basic Edge Services

You can configure basic services, such as DHCP and DNS, on each deployed vShield Edge appliance.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- Primary DNS server address ________________________

1. Click the **HQ-Edge > Settings** button.
2. Locate the DNS Configuration section and click the **Change** link.
3. In the Change DNS configuration panel, configure the HQ-Edge DNS service parameters.

Option	Action
Enable DNS service	Select the check box.
DNS Server 1	Type the Primary DNS server address in the text box.
DNS Server 2	Leave blank.
Cache Size	Leave the default of `16`.
Enable Logging	Leave the check box deselected.

4. Click **OK**.
5. At the top of the page, click the **DHCP** button.
6. In the DHCP Pools section, click the **Add** (green plus symbol) icon.
7. In the Add DHCP Pool panel, configure a DHCP pool for the Shared Network virtual wire interface.

Option	Action
Auto Configure DNS	Select the check box.
Lease never expires	Select the check box.
Start IP	Type **`192.168.1.100`** in the text box.
End IP	Type **`192.168.1.199`** in the text box.

Option	Action
Domain Name	Type **`vclass.local`** in the text box.
Default Gateway	Type **`192.168.1.1`** in the text box.

8. Click the **Add** button.
9. In the top section, select the **Enable logging** check box.
10. Click the **Enable** button to enable the DHCP service.
11. Click the **Publish Changes** button, near the upper-right corner of the page, in the green bar.
12. Click the **blue back-arrow** icon.

Task 8: Examine Changes in vSphere

Deployed vShield Edge appliances are accessible in the inventory of the hosting cluster.

Student B performs this task. Student A verifies the settings.

1. In the Firefox window, click the **vSphere Web Client** tab.
2. In the left pane, click the **Hosts and Clusters** icon.
3. Click the **refresh** icon, located left of the logged-in user name at the top of the page.
4. In the inventory tree, select the **HQ** > **HQ Infrastructure** > **HQ-Edge-0** virtual machine item.
5. In the right pane, click the **Summary** tab.
6. Use the vertical scroll bar to examine the VM Hardware information and verify the following.
   - The appliance was deployed with `1 CPU(s)`.
   - The appliance was deployed with `256MB` of memory.
   - The appliance has 10 network adapters.
   - Network adapter 1 is connected to `pg-HQ-External`.
   - Network adapter 2 is connected to a VXLAN virtual wire port group.

Task 9: Test Basic Services and Verify External Network Connectivity

When deploying new vShield Edge appliances or configuring new services for the virtual networks, a best practice is to test each feature and verify connectivity.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- Client administrator user name ________________________
- Standard lab password ________________________
- HQ network gateway address ________________________

1. In the vSphere Hosts and Clusters inventory tree, select the **HQ > HQ Application > Web3** virtual machine item.
2. In the center pane, select **Open Console** from the **Actions** drop-down menu.
3. If you are prompted to log in to the client machine, perform the following actions.
   a. Click the **Send Ctrl-Alt-Delete** button in the upper-right corner of the page.
   b. Log in as the client administrator, using the standard lab password.
4. On the client desktop, double-click the **Use-DHCP.bat** icon.
5. When prompted, press any key to reconfigure the client to use DHCP.
6. After the operation completes, press any key to close the script window.
7. On the client desktop, double-click the **Command Prompt** shortcut.
8. In the Command Prompt window, examine the client IP configuration by typing the following command.

   ```
   ipconfig /all
   ```

9. Use the `ipconfig` command output to verify the following values.
   - The client IP address is within the DHCP pool range of `192.168.1.100-192.168.1.199`.
   - The default gateway IP address is `192.168.1.1`.
   - The DNS server list includes the IP address `192.168.1.1`.
   - The DHCP server IP address is `192.168.1.1`.

   NOTE

   You might experience a delay when the first DHCP operation is performed. If the host IP address shown is 0.0.0.0, wait 1 minute, and perform steps 14 and 15 again.

10. Test connectivity between the VXLAN virtual wire and the external network by pinging the HQ Production network gateway address.

    ```
    ping 172.20.11.10
    ```

    NOTE

    The ping test generates responses from the gateway, which is the upstream router. The router has been preconfigured with the necessary static routes to return traffic to the Shared Network virtual wire through the external interface of the deployed vShield Edge appliance.

11. Test DNS resolution and Internet connectivity by pinging the VMware web site.

    ```
    ping www.vmware.com
    ```

12. Close the Command Prompt window.
13. In the Firefox window, close the **Web3** virtual machine tab.
14. Click the **vShield Manager** tab.

Lab 7

Transforming IP Packet Addressing by Using NAT Rules

Objective: Create DNAT and SNAT rules to establish bidirectional connectivity through an external 1:1 address mapping

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Connect a Virtual Wire to a Deployed vShield Edge Appliance
3. Power On the Web1 Virtual Machine and Establish Connectivity to the vShield Edge Appliance
4. Add IP Addresses to the vShield Edge External Interface
5. Create a DNAT Rule to Enable External Access to the Client Server
6. Test Inbound Access Through the DNAT Rule
7. Create an SNAT Rule and Test Outbound Connectivity

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing class from the previous lab, skip to the next task.

Student B performs this task. Student A verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the vSphere administrator, using the standard lab password.
4. In the vSphere Web Client interface, navigate to **vCenter > Hosts and Clusters**.
5. Power on the following virtual machines.
    - Branch > Branch Application > Web4
    - HQ > HQ Application > Web3
6. In the Firefox window, open a new browser tab.
7. Click the **vShield Manager** favorite link.
8. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.
9. In the left pane, expand the **Datacenters** container and select **Datacenter-A**.
10. In the right pane, click the **Network Virtualization** tab.

Task 2: Connect a Virtual Wire to a Deployed vShield Edge Appliance

Each VMware® vShield Edge™ appliance can connect to many different VXLAN virtual wires.

Student B performs this task. Student A verifies the settings.

1. In the edges list, select the **HQ-Edge** instance.
2. Click the **Actions** menu and select **Manage**.
3. Click the **HQ-Edge > Configure** button.
4. In the list, select the **vnic2** interface item.
5. Click the **Edit** (pencil) icon.

6. In the Edit Edge Interface panel, perform the following actions.

   a. Type **`HQ Network`** in the **Name** text box.

   b. For Type, leave the **Internal** radio button selected.

   c. Click the **Select** link located to the right of the **Connected To** text box.

   d. In the Connect Edge to a Network panel, select the **HQ Network** radio button and click **Select**.

   e. Under Configure Subnets, click the **Add** (green plus symbol) icon.

   f. In the **Add Subnet** panel, click the **Add** (green plus symbol) icon to configure the IP address and subnet of the HQ-Edge interface that connects to the HQ Network virtual wire.

Option	Action
IP Address	Type **`192.168.20.1`** in the **IP Address** text box and click **OK.**
Subnet Mask	Type **`255.255.255.0`** in the text box and click **Save.**

   g. Use the vertical scroll bar to find the MTU setting and verify that the MTU is set to `1500`.

   h. Click **Save**.

Task 3: Power On the Web1 Virtual Machine and Establish Connectivity to the vShield Edge Appliance

Power on a guest virtual machine that is connected to the HQ Network.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- Client administrator user name ______________________________
- Standard lab password ______________________________

1. In the Firefox window, click the **vSphere Web Client** tab.
2. In the left pane, select the **HQ** > **HQ Application** > **Web1** virtual machine item.
3. In the middle pane, select **Power On** from the **Actions** drop-down menu.
4. When the power-on operation completes, select **Open Console** from the **Actions** menu.

5. When prompted to log in, perform the following actions.
   a. Click the **Send Ctrl-Alt-Delete** button located in the upper-right corner of the page.
   b. Log in as the client administrator, using the standard lab password.
6. On the Web1 desktop, double-click the **Local Area Connection** shortcut.
7. In the Local Area Connection Status window, click the **Properties** button.
8. In the Local Area Connection Properties window, select **Internet Protocol (TCP/IP)** and click the **Properties** button.
9. In the Internet Protocol (TCP/IP) Properties window, perform the following actions.
   a. In **Default Gateway address**, type **`192.168.20.1`**.
   b. In **Preferred DNS server address**, type **`192.168.20.1`**.
   c. Click **OK**.
10. Close the Local Area Connection Properties window.
11. Close the Local Area Connection Status window.
12. On the Web1 desktop, double-click the **Command Prompt** shortcut.
13. In the Command Prompt window, verify connectivity to the vShield Edge appliance by typing the following command.

```
ping 192.168.20.1
```

14. Verify that the client machine does not have connectivity beyond the edge appliance by pinging the upstream router on the external segment.

```
ping 172.20.11.10
```

NOTE

Each ping request times out. The upstream router has not been configured with the static routes necessary to direct response traffic back to the HQ Network virtual wire. This behavior is correct for this lab. DNAT rules will be configured to associate the virtual machine private IP address with an external segment address.

15. Close the Command Prompt window.
16. On the Web1 desktop, double-click the **Internet Explorer** shortcut.
17. In the Internet Explorer window, examine the Web1 Web page by navigating to http://localhost.
18. Verify that Web page reports a server IP address of `192.168.20.10`.
19. Close the Internet Explorer window.

Task 4: Add IP Addresses to the vShield Edge External Interface

The addresses to be transformed by a DNAT rule must be added to the appropriate vShield Edge interface. The vShield Edge appliance performs proxy-ARP operations for each address configured on an interface.

Student B performs this task. Student A verifies the settings.

1. In the Firefox window, click the **vShield Manager** tab.
2. Click the **HQ-Edge > Configure** button.
3. In the edge interface list, select the **External** interface item.
4. Click the **Edit** (pencil) icon.
5. In the Edit Edge Interface panel, under **Configure Subnets**, select the `172.20.11.11` IP address item.
6. Click the **Edit** (pencil) icon.
7. In the Edit Subnet panel, click the **Add** (green plus symbol) icon to add the IP address to be used for external NAT operations.

Option	Action
IP Address	Type **`172.20.11.12`** in the **IP Address** text box and click **OK**.

8. Click **Save** to close the Edit Subnet panel.
9. Click **Save** to close the Edit Edge Interface panel.
10. In the interface list, verify that the following IP addresses are defined for the External interface.
    - 172.20.11.11, with an asterisk (*) indicating primary IP address
    - 172.20.11.12

Task 5: Create a DNAT Rule to Enable External Access to the Client Server

DNAT rules can be defined for any IP address or range of IP addresses that have been configured on an edge network interface.

Student A performs this task. Student B verifies the settings.

1. Click the **HQ-Edge > NAT** button.
2. Click the **Add** (green plus symbol) icon and select **Add DNAT Rule**.
3. In the Add DNAT Rule panel, configure the following settings.

Option	Action
Applied On	Select External from the drop-down menu.
Original IP/Range	Type **`172.20.11.12`** in the text box.
Protocol	Type **`any`** in the text box.
Original Port/Range	Leave blank.
Translated IP/Range	Type the Web1 server IP address of **`192.168.20.10`** in the text box.
Translated Port/Range	Leave blank.
Description	Leave blank.
Enabled	Select the check box.
Enable logging	Select the check box.

4. Click the **Add** button.
5. Click the **Publish Changes** button, located above the upper-right corner of the NAT rule list, in the green bar.

Task 6: Test Inbound Access Through the DNAT Rule

A DNAT rule associates one destination address with a different destination address. Solicited response traffic is automatically mapped back through the DNAT rule in reverse. Unsolicited outbound traffic does not traverse a DNAT rule.

Student B performs this task. Student A verifies the settings.

1. In the Firefox window, open a new browser tab.
2. Click the **Web1-DNAT** favorite link.

   NOTE

   The Web page hosted on the Web1 virtual machine is displayed.

3. Verify that the browsed URL is `172.20.11.12` and that the responding Web server reports a server IP address of `192.168.20.10 (web1)`.
4. Close the browser tab.

Task 7: Create an SNAT Rule and Test Outbound Connectivity

An SNAT rule is used to transform packet source addresses. Transformed traffic will traverse the vShield Edge appliance and appear as originating from the new source subnet.

Student A performs this task. Student B verifies the settings.

1. In the Firefox window, click the **Web1** tab.
2. On the Web1 desktop, double-click the **Command Prompt** shortcut.
3. Verify that there is no connectivity beyond the edge device by typing the following command to ping the upstream router.

   ```
   ping 172.20.11.10
   ```

   NOTE

   The ping requests time out. Routes identifying the HQ Network (192.168.20.0/24) are not defined on the upstream router.

4. In the Firefox window, click the **vShield Manager** tab.
5. In the HQ-Edge > NAT view, click the **Add** (green plus symbol) icon and select **Add SNAT Rule**.

6. In the Add SNAT Rule panel, configure the following settings.

Option	Action
Applied On	Select **External** from the drop-down menu.
Original Source IP/Range	Type the Web1 server IP address of `192.168.20.10` in the text box.
Translated Source IP/Range	Type `172.20.11.12` in the text box.
Description	Leave blank.
Enabled	Select the check box.
Enable logging	Select the check box.

7. Click the **Add** button.
8. Click the **Publish Changes** button, located above the upper-right corner of the NAT rule list, in the green bar.
9. In the Firefox window, click the **Web1** tab.
10. Click the Command Prompt window.
11. Verify connectivity beyond the edge device by typing the following command to ping the upstream router.

    ```
    ping 172.20.11.10
    ```

    NOTE

    Replies are received from the upstream router. The upstream router is replying to the translated IP address. When the client virtual machine sends the ping requests, the source IP address of each ICMP packet is translated to the public/external NAT address defined by the SNAT rule. Effectively, the upstream router is responding to ping requests from the 172.20.11.12 IP address.

12. Close the Command Prompt window.
13. In the Firefox window, close the Web1 tab.
14. Click the **vShield Manager** tab.
15. Click the **blue back-arrow** icon.

Lab 8
Configuring Firewall Rules

Objective: Create firewall rules to restrict inbound traffic to allow HTTP and FTP while denying all other protocols

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Create an IP Address Set for DNAT-Accessible Addresses
3. Create a Firewall Rule to Block All Inbound Traffic to DNAT Addresses
4. Create a Service Group
5. Create a Firewall Rule to Allow Web Protocols to DNAT Addresses
6. Configure Connectivity for a Route-Accessible Web Server
7. Create an IP Address Set to Identify a Host on a Route-Accessible Virtual Wire
8. Change the Existing Rule Scope to Include Additional Hosts

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing class from the previous lab, skip to the next task.

Student B performs this task. Student A verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the VMware® vSphere® administrator, using the standard lab password.
4. In the vSphere Web Client interface, navigate to **vCenter > Hosts and Clusters**.
5. Power on the following virtual machines.
   - Branch > Branch Application > Web4
   - HQ > HQ Application > Web1
   - HQ > HQ Application > Web3
6. In the Firefox window, open a new browser tab.
7. Click the **vShield Manager** favorite link.
8. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.
9. In the left pane, expand the **Datacenters** container and select **Datacenter-A**.
10. In the right pane, click the **Network Virtualization** tab.

Task 2: Create an IP Address Set for DNAT-Accessible Addresses

An IP address set identifies the source or destination addresses to be used in a firewall rule.

Student B performs this task. Student A verifies the settings.

1. On the Network Virtualization tab, select the **HQ-Edge** item.
2. Click the **Actions** drop-down menu and select **Manage**.
3. Click the **HQ-Edge > Configure** button.
4. Click the **Grouping Objects** link.
5. Click the **Add** (green plus symbol) icon and select **IP Addresses**.

6. In the Add IP Addresses panel, configure the DNAT-accessible address set.

Option	Action
Name	Type **`DNAT-addresses`** in the text box.
Description	Leave blank.
IP Addresses	Type **`172.20.11.12`** in the text box.

7. Click **OK**.

Task 3: Create a Firewall Rule to Block All Inbound Traffic to DNAT Addresses

When defining firewall rules for hosts that are accessible through DNAT rules, the rule must specify the DNAT external addresses and not the internal host addresses.

Student A performs this task. Student B verifies the settings.

1. Click the **HQ-Edge > Firewall** button.
2. Click the **Add** (green plus symbol) icon.

   A new rule highlighted in blue is added to the rules list.
3. Configure the new firewall rule by performing the following actions.

   Use the horizontal scroll bar to reposition the display as each column is configured.

   a. Point to the **Name** cell and click the **plus symbol** icon.

   b. In the Rule Name panel, type **`Deny Inbound`** and click **OK**.

   c. Point to the **Destination** cell and click the **plus symbol** icon.

   d. In the input panel, select the **DNAT-addresses** check box and click **OK**.

   e. Point to the **Action** cell and click the **plus symbol** icon.

   f. In the input panel, select the **Deny** and **Log** radio buttons and click **OK**.
4. Click the **Publish** button, located above the upper-right corner of the rules list, in the green bar.
5. In the Firefox window, open a new tab.
6. Click the **Web1-DNAT** favorite link.
7. If the Web page hosted by the Web1 server is displayed, click the page refresh icon to flush the cache and force the page to reload.
8. Verify that the Web page does not load and close the browser tab.

Task 4: Create a Service Group

A service group is a collection of network services that are applied to a single firewall rule.

Student B performs this task. Student A verifies the settings.

1. In the Firefox window, click the **vShield Manager** tab.
2. Click the **HQ-Edge > Configure** button.
3. Click the **Services** link.
4. Click the **Add** (green plus symbol) icon and select **Service Group**.
5. In the Add Service Group panel, configure the Allowed-web-protocols service group settings.
   a. Type **`Allowed-web-protocols`** in the Name text box.
   b. Leave the **Description** text box blank.
   c. Click the **Name** column heading to sort the list by name.
   d. Scroll down to locate the FTP service.
   e. Select the **FTP** service check box.
   f. Scroll down to locate the HTTP service.
   g. Select the **HTTP** service check box.
6. Click **OK**.

Task 5: Create a Firewall Rule to Allow Web Protocols to DNAT Addresses

Using rule precedence, firewall rules can be sequenced to handle complex conditions.

Student A performs this task. Student B verifies the settings.

1. Click the **HQ-Edge > Firewall** button.
2. Click the **Add** (green plus symbol) icon.

   A new rule is added to the rules list, highlighted in blue.
3. Configure the new firewall rule by performing the following actions.

   Use the horizontal scroll bar to reposition the display as each column is configured.

   a. Point to the **Name** cell and click the **plus symbol** icon.
   b. In the Rule Name panel, type **`Allowed Inbound Web`** and click **OK**.
   c. Point to the **Destination** cell and click the **plus symbol** icon.

   d. In the input panel, select the **DNAT-addresses** check box and click **OK**.
   e. Point to the **Service** cell and click the **plus symbol** icon.
   f. In the input panel, select the **Allowed-web-protocols** check box and click **OK**.
   g. Point to the **Action** cell and click the **plus symbol** icon.
   h. In the input panel, select the **Log** radio buttons and click **OK**.

4. Use the **Move Rule Up** and **Move Rule Down** icons to move the Allowed Inbound Web rule so that it precedes the Deny Inbound rule, if needed.
5. Click the **Publish** button, located above the upper-right corner of the rules list, in the green bar.
6. In the Firefox window, open a new browser tab.
7. Click the **Web1-DNAT** favorite link.
8. After the Web page is displayed, close the browser tab.

Task 6: Configure Connectivity for a Route-Accessible Web Server

In the lab environment, the upstream router has been configured with a static route for the Shared Network virtual wire. The HQ and Branch networks are not accessible through static routes.

Student B performs this task. Student A verifies the settings.

Use the following information from the class configuration handout:

- Client administrator user name _________________________
- Standard lab password _________________________

1. In the Firefox window, click the **vSphere Web Client** tab.
2. In the Hosts and Clusters inventory panel, select the **Branch > Branch Application > Web4** virtual machine item.
3. In the center pane, select **Open Console** from the **Actions** drop-down menu.
4. If prompted to log in to the Web4 virtual machine, perform the following actions.
   a. Click the **Send Ctrl-Alt-Delete** button in the upper-left corner of the console page.
   b. Log in as the client administrator, using the standard lab password.
5. On the Web4 desktop, double-click the **Use-Static.bat** icon.
6. When prompted, press any key to continue.

   The script executes a series of commands to establish full network connectivity.

7. Use the script output to verify the following configuration values.
   - The client IP address is **`192.168.1.200`**.
   - The default gateway is **`192.168.1.1`**.
   - The DNS server list includes **`192.168.1.1`**.
8. Close the Command Prompt window.
9. Close the Web4 browser tab.

Task 7: Create an IP Address Set to Identify a Host on a Route-Accessible Virtual Wire

Additional address sets can be added to existing firewall rules to broaden the source and destination scopes.

Student A performs this task. Student B verifies the settings.

1. In the Firefox window, click the **vShield Manager** tab.
2. Click the **HQ-Edge > Configure** button.
3. Click the **Grouping Objects** link.
4. Click the **Add** (green plus symbol) icon and select **IP Addresses**.
5. In the Add IP Addresses panel, configure the Route-accessible-hosts address set.

Option	Action
Name	Type **`Route-accessible-hosts`** in the text box.
Description	Leave blank.
IP Addresses	Type **`192.168.1.200`** in the text box.

6. Click **OK**.

Task 8: Change the Existing Rule Scope to Include Additional Hosts

Additional address sets can be added to existing firewall rules to broaden the source and destination scope.

Student B performs this task. Student A verifies the settings.

1. Click the **HQ-Edge > Firewall** button.
2. In the firewall rules list, select the **Deny Inbound** rule.
3. Point to the **Destination** cell and click the **plus symbol** icon.
4. In the input panel, select the **Route-accessible-hosts** check box and click **OK**.
5. Click the **Publish** button, located above the upper-right corner of the rules list, in the green bar.
6. In the Firefox window, open a new browser tab.
7. Click the **Web4-Routed** favorite link.
8. Verify that the Web page cannot be loaded and close the browser tab.
9. In the firewall rules list, select the **Allowed Inbound Web** rule.
10. Point to the **Destination** cell and click the **plus symbol** icon.
11. In the input panel, select the **Route-accessible-hosts** check box and click **OK**.
12. Click the **Publish** button, located above the upper-right corner of the rules list, in the green bar.
13. In the Firefox window, open a new browser tab.
14. Click the **Web4-Routed** favorite link.
15. After the Web4 Web page is displayed, close the browser tab.
16. In the vShield Manager interface, click the **blue back-arrow** button.

Lab 9

Configuring an IPsec Tunnel

Objective: Configure an IPsec VPN tunnel to enable network communication between virtual wires created on different clusters

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Create a Port Group for External Access
3. Create an Edge for the Branch Network Virtual Wire
4. Deploy an Edge Appliance to the Branch Cluster
5. Add an Internal Interface for the Branch Virtual Wire
6. Configure an IPsec Tunnel Endpoint on the Branch Cluster Edge Appliance
7. Configure an IPsec Tunnel Endpoint on the HQ Cluster Edge Appliance
8. Test IPsec Tunnel Connectivity
9. Examine the Channel and Tunnel Status

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing class from the previous lab, skip to the next task.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the vSphere administrator, using the standard lab password.
4. In the vSphere Web Client interface, navigate to **vCenter > Hosts and Clusters**.
5. Power on the following virtual machines.
    - Branch > Branch Application > Web4
    - HQ > HQ Application > Web1
    - HQ > HQ Application > Web3
6. In the Firefox window, open a new browser tab.
7. Click the **vShield Manager** favorite link.
8. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.
9. In the left pane, expand the **Datacenters** container and select **Datacenter-A**.
10. In the right pane, click the **Network Virtualization** tab.

Task 2: Create a Port Group for External Access

A port group that has not been allocated for VXLAN virtual wires must be available to provide external network access to each VMware® vShield Edge™ uplink interface.

Student A performs this task. Student B verifies the settings.

1. In the Firefox window, click the **vSphere Web Client** tab.
2. In the left pane, click the **Networking** icon.
3. Select the **dvs-Branch-Production** distributed switch item.

4. In the center pane, select **New Distributed Port Group** from the **Actions** drop-down menu.
5. In the New Distributed Port Group panel, type **`pg-Branch-External`** in the **Name** text box and click **Next**.
6. Under Configure settings, click **Next** to accept all default configuration values.
7. Under Ready to complete, click **Finish**.

Task 3: Create an Edge for the Branch Network Virtual Wire

A vShield Edge is first defined as an appliance configuration that includes up to 10 network interfaces.

Student B performs this task. Student A verifies the settings.

Use the following information from the class configuration handout:

- vSphere administrator user name _________________________
- Standard lab password _________________________
- Branch network gateway address _________________________

1. In the Firefox window, click the **vShield Manager** tab.
2. Above the edge list, click the **Add** (green plus symbol) icon.
3. In the Add Edge panel, under Name & Description, provide the following Branch-Edge settings.

Option	Action
Name	Type **`Branch-Edge.`**
Hostname	Leave blank.
Description	Leave blank.
Tenant	Leave blank.
Enable HA	Leave deselected.

4. Click **Next**.

5. Under CLI Credentials, provide the following SSH access settings.

Option	Action
User Name	Keep the default of admin.
Password	Type the standard lab password.
Enable SSH access	Select the check box.

6. Click **Next**.
7. Under Edge Appliances, click **Next**.

   You deploy an appliance in another task.
8. Under Interfaces, click the **Add** (green plus symbol) icon.
9. In the Add Edge Interface panel, perform the following actions.
   a. Type **`External`** in the **Name** text box.
   b. For type, leave the **Uplink** radio button selected.
   c. Select **pg-Branch-External** from the **Connected To** drop-down menu.
   d. For Connectivity Status, leave the **Connected** radio button selected.
   e. Under Configure Subnets, click the **Add** (green plus symbol) icon.
   f. In the Add Subnet panel, configure the IP address and subnet for the Branch-Edge external interface.

Option	Action
IP Address	Click the **Add** (green plus symbol). Type **`172.20.110.11`** in the text box. Click **OK**.
Subnet Mask	Type **`255.255.255.0`** in the text box. Click **Save**.

   g. Use the vertical scroll bar to find the MTU setting and verify that the MTU is set to `1500`.
   h. Click the **Add** button.

10. Click **Next**.
11. Under Default Gateway, configure the next hop settings for the Branch-Edge external interface.

Option	Action
Configure Default Gateway	Select the check box.
vNIC	Leave **External** selected.
Gateway IP	Type the Branch production network gateway address in the text box.
MTU	Verify that the MTU is `1500`.

12. Click **Next**.
13. Under Firewall & HA, provide the following default policy settings.

Option	Action
Configure Firewall default policy	Select the check box.
Default Traffic Policy	Select the **Accept** radio button.
Logging	Select the **Enable** check box.

14. Click **Next**.
15. Under Summary, click **Finish**.

Task 4: Deploy an Edge Appliance to the Branch Cluster

When a vShield Edge appliance is deployed, the hosting cluster and the datastore must be specified. Cluster selection limits which VXLAN virtual wires can be attached to the appliance.

Student A performs this task. Student B verifies the settings.

1. In the edge list, select the **Branch-Edge** instance.
2. Click the **Actions** drop-down menu, and select **Manage**.
3. Use the vertical scroll bar to find the **Edge Appliances** section at the bottom of the settings page.
4. Under Edge Appliances, click the **Add** (green plus symbol) icon.
5. In the Add Edge Appliance panel, select the cluster and datastore that will host the Branch-Edge appliance.

Option	Action
Cluster/Resource Pool	Select Branch Infrastructure from the drop-down menu.
Datastore	Select Shared-Datastore from the drop-down menu.

6. Click **Add**.
7. Use the vertical scroll bar to move to the top of the settings page.
8. Monitor the current job status to completion.

Task 5: Add an Internal Interface for the Branch Virtual Wire

After VXLAN virtual wires are deployed to a specific cluster, they can be attached to available vShield Edge appliance network interfaces.

Student B performs this task. Student A verifies the settings.

1. Click the **Branch-Edge** > **Configure** button.
2. In the interface list, select the **vnic1** interface item.
3. Click the **Edit** (pencil) icon.
4. In the Edit Edge Interface panel, perform the following actions.
   a. Type **`Branch Network`** in the **Name** text box.
   b. For Type, leave the **Internal** radio button selected.
   c. Click the **Select** link, located to the right of the **Connected To** text box.

d. In the Connect Edge to a Network panel, select the **Branch Network** radio button and click **Select**.

e. For Connectivity Status, leave the **Connected** radio button selected.

f. Under Configure Subnets, click the **Add** (green plus symbol) icon.

g. In the Add Subnet panel, configure the IP address and subnet for the Branch-Edge interface that connects to the Branch Network virtual wire.

Option	Action
IP Address	Click the **Add** (green plus symbol) icon. Type **`192.168.30.1`** in the **IP Address** text box. Click OK.
Subnet Mask	Type **`255.255.255.0`** in the text box. Click **Save**.

h. Use the vertical scroll bar to find the MTU setting and verify that the MTU is set to `1500`.

i. Click **Save**.

Task 6: Configure an IPsec Tunnel Endpoint on the Branch Cluster Edge Appliance

An IPsec VPN tunnel is configured between two participating vShield Edge appliances, also called peers. Each participating appliance must be configured separately.

Student A performs this task. Student B verifies the settings.

1. Click the **Branch-Edge** > **VPN** button.
2. Below the function buttons, verify that the **IPSec VPN** link is selected.
3. In the IPSec VPN tunnel list, click the **Add** (green plus symbol) icon.
4. In the Add IPSec VPN panel, configure the Branch-Edge appliance as a tunnel peer.

Option	Action
Name	Type **`HQ-Branch Tunnel`** in the text box.
Local Id	Type **`Branch`** in the text box.

Option	Action
Local Endpoint	Type **`172.20.110.11`** in the text box.
Local Subnets	Type **`192.168.30.0/24`** in the text box.
Peer Id	Type **`HQ`** in the text box.
Peer Endpoint	Type **`172.20.11.11`** in the text box.
Peer Subnets	Type **`192.168.20.0/24`** in the text box.
Encryption Algorithm	Leave **AES** selected.
Authentication	Leave **PSK** selected.
Pre-Shared Key	Type **`vmware1!`** in the text box.
Diffie-Hellman Group	Leave **DH2** selected.
MTU	Leave the default of **`1500`**.
Enable perfect forward secrecy (PFS)	Leave the check box selected.

5. Click **OK**.
6. Click the **Enable** button to enable the IPsec VPN service.
7. Click the **Publish Changes** button, located near the upper-right corner of the page, in the green bar.

Task 7: Configure an IPsec Tunnel Endpoint on the HQ Cluster Edge Appliance

An IPsec VPN tunnel is created between two participating vShield Edge appliances called peers. Each participating appliance must be configured separately, with the Local and Peer information exchanged.

Student B performs this task. Student A verifies the settings.

1. Click the **blue back-arrow** icon.
2. In the edge list, select the **HQ-Edge** item.
3. Click the **Actions** menu and select **Manage**.
4. Click the **HQ-Edge > VPN** button.

5. In the IPSec VPN tunnels list, click the **Add** (green plus symbol) icon.
6. In the Add IPSec VPN panel, configure the HQ-Edge appliance as a tunnel peer.

Option	Action
Name	Type **`HQ-Branch Tunnel`** in the text box.
Local Id	Type **`HQ`** in the text box.
Local Endpoint	Type **`172.20.11.11`** in the text box.
Local Subnets	Type **`192.168.20.0/24`** in the text box.
Peer Id	Type **`Branch`** in the text box.
Peer Endpoint	Type **`172.20.110.11`** in the text box.
Peer Subnets	Type **`192.168.30.0/24`** in the text box.
Encryption Algorithm	Leave **AES** selected.
Authentication	Leave **PSK** selected.
Pre-Shared Key	Type **`vmware1!`** in the text box.
Diffie-Hellman Group	Leave **DH2** selected.
MTU	Leave the default of **`1500`**.
Enable perfect forward secrecy (PFS)	Leave the check box selected.

7. Click **OK**.
8. Click the **Enable** button to enable the IPsec VPN service.
9. Click the **Publish Changes** button, located near the upper-right corner of the page, in the green bar.

Task 8: Test IPsec Tunnel Connectivity

After an IPsec tunnel is configured on each peer, it is automatically established.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- Client administrator user name ________________________
- Standard lab password ________________________

1. In the Firefox window, select the **vSphere Web Client** tab.
2. In the left panel, click the **Hosts and Clusters** icon.
3. In the inventory tree, select the **Branch** > **Branch Application** > **Web5** virtual machine item.
4. In the center pane, select **Power On** from the **Actions** drop-down menu.
5. After the power operation completes, select **Open Console** from the **Actions** drop-down menu.
6. When prompted to log in, click the **Send Ctrl-Alt-Delete** button in the upper-right corner of the page.
7. Log in as the client administrator, using the standard lab password.
8. On the client desktop, double-click the **Command Prompt** shortcut.
9. In the Command Prompt window, examine the client IP settings by executing the following command.

   ```
   ipconfig /all
   ```
10. Use the **`ipconfig`** output to verify the following.
    - The client IP address is `192.168.30.10`.
    - The client subnet mask is `255.255.255.0`.
    - The default gateway is `192.168.30.1`, the Branch edge appliance.
11. Test tunnel connectivity by typing the following command to ping a virtual machine attached to the HQ Network virtual wire.

    ```
    ping 192.168.20.10
    ```
12. Close the Command Prompt window.
13. On the client desktop, double-click the **Internet Explorer** shortcut.
14. In Internet Explorer, browse to the Web page hosted by the HQ Network VM.

    ```
    http://192.168.20.10
    ```

15. Verify that the Web page reports the same address as browsed.
16. Close the Internet Explorer window.
17. In the Firefox window, close the Web5 tab.

Task 9: Examine the Channel and Tunnel Status

For each defined tunnel, the status of the tunnel and channel can be determined by examining the IPsec tunnel configuration for each participating endpoint.

Student B performs this task. Student A verifies the settings.

1. In the Firefox window, click the **vShield Manager** tab.
2. Click the **blue back-arrow** icon.
3. In the edge list, select the **Branch-Edge** item.
4. Click the **Actions** drop-down menu and select **Manage**.
5. Click the **Branch-Edge** > **VPN** button.
6. Wait for the page refresh to occur.

   The pointer changes from a clock icon to the standard pointer when the refresh is complete.
7. For the **HQ-Branch Tunnel** item, verify the following.
   - The Channel Status field contains a green check mark.
   - The Tunnel Status field shows `1 UP 0 DOWN`.
8. Click the **blue back-arrow** button.

Lab 10

Configuring SSL VPN-Plus

Objective: Configure SSL-VPN to enable private network access

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Configure SSL VPN-Plus Server Settings
3. Configure a Local Authentication Server and a Local User
4. Enable SSL VPN-Plus and Test Portal Access
5. Configure an IP Pool and Private Networks
6. Create and Install an Installation Package
7. Test Network Access by Using the SSL VPN-Plus Client Application

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing class from the previous lab, skip to the next task.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the vSphere administrator, using the standard lab password.
4. In the vSphere Web Client interface, navigate to **vCenter > Hosts and Clusters**.
5. Power on the following virtual machines.
    - Branch > Branch Application > Web4
    - Branch > Branch Application > Web5
    - HQ > HQ Application > Web1
    - HQ > HQ Application > Web3
6. In the Firefox window, open a new browser tab.
7. Click the **vShield Manager** favorite link.
8. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.
9. In the left pane, expand the **Datacenters** container and select **Datacenter-A**.
10. In the right pane, click the **Network Virtualization** tab.

Task 2: Configure SSL VPN-Plus Server Settings

The IP address used by SSL VPN-Plus must be configured on the VMware® vShield Edge™ external interface, and can be the primary or any secondary address.

Student A performs this task. Student B verifies the settings.

1. In the edge list, select the **HQ-Edge** item.
2. Click the **Actions** menu and select **Manage**.
3. Click the **HQ-Edge > VPN** button.

4. Click the **SSL VPN-Plus** link.
5. In configuration categories list, click **Server Settings**.
6. Click the **Change** button located on the right side of the page.
7. In the Change Server Settings panel, configure the HQ-Edge external IP address as the tunnel endpoint.

Option	Action
IP Address	Leave **172.20.11.11 (Primary)** selected.
Port	Leave the default of `443`.
Cipher List	Leave **RC4-MD5** selected.
Server Certificate	Leave the **Use Default Certificate** check box selected.

8. Click **OK** and wait for the update to complete.

Task 3: Configure a Local Authentication Server and a Local User

SSL VPN-Plus supports several authentication methods. For this lab, you will be configuring a local authentication server and a local user.

Student B performs this task. Student A verifies the settings.

1. In the configuration categories list, click **Authentication**.
2. Click the **Add** (green plus symbol) icon.
3. In the **Add Server** panel, configure a local authentication server.

Option	Action
Type	Select **Local** from the drop-down menu.
Password Policy	Leave the check box selected.
Password Length	Leave the defaults of `1 To 63`.
Minimum no. of alphabets	Type **6** in the text box.
Minimum no. of Digits	Leave blank.
Minimum no. of special characters	Leave blank.

Option	Action
Password should not contain user ID	Leave the check box deselected.
Password expires in	Leave the default of `30 days`.
Expiry notification in	Leave the default of `25 days`.
Account Lockout Policy	Deselect the check box.
Status	Leave the **Enabled** radio button selected.
Use this server for secondary authentication	Leave the check box deselected.

4. Click **OK**.
5. In the configuration categories list, click **Users**.
6. Click the **Add** (green plus symbol) icon.
7. In the Add User panel, configure a new local user account.

Option	Action
User ID	Type **`vpnuser`** in the text box.
Password	Type **`vmware1!`** in the text box.
Re-type Password	Type **`vmware1!`** in the text box.
First Name	Leave blank.
Last Name	Leave blank.
Description	Leave blank.
Password never expires	Select the check box.
Allow change password	Leave the check box selected.
Change password on next login	Leave the check box deselected.
Status	Leave the **Enabled** radio button selected.

8. Click **OK**.

Task 4: Enable SSL VPN-Plus and Test Portal Access

SSL VPN-Plus portal access can be tested after the server settings and authentication are configured. Student A performs this task. Student B verifies the settings.

1. In the configuration categories list, click **Dashboard**.
2. In the Status box, click the **Enable** button.
3. When prompted to enable the service, click **Yes** and wait for the update to complete.
4. In the Firefox window, open a new browser tab.
5. Click the **SSL VPN-Plus** shortcut link.
6. Click the **I Understand the Risks** link.
7. Click the **Add Exception** button.
8. In the Add Security Exception dialog, click the **Confirm Security Exception** button.
9. When prompted to log in, type the user name and password of the local user account created in the preceding task.
   - User name: `vpnuser`
   - Password: `vmware1!`
10. Verify that the following tab appears in the upper-left corner of the SSL VPN-Plus Web portal under the branding graphic.
    - Tools
11. Click the Logout link, located in the upper-right corner of the Web portal page, in the black bar.
12. When prompted, click **OK**.
13. Close the browser tab.

Task 5: Configure an IP Pool and Private Networks

Each SSL VPN-Plus client is assigned an IP address from a virtual subnet and is granted access to specific private subnets.

Student B performs this task. Student A verifies the settings.

1. In the configuration categories list, click **IP Pool**.
2. Click the **Add** (green plus symbol) icon.
3. In the Add IP Pool panel, configure the virtual subnet used by SSL VPN-Plus clients to access internal resources.

Option	Action
IP Range	Type **`192.168.200.2`** in the first text box. Type **`192.168.200.254`** in the second text box.
Netmask	Type **`255.255.255.0`** in the text box.
Gateway	Type **`192.168.200.1`** in the text box.
Description	Leave blank.
Status	Leave the **Enabled** radio button selected.
Primary DNS	Leave blank.
Secondary DNS	Leave blank.
DNS Suffix	Leave blank.
WINS Server	Leave blank.

4. Click **OK**.
5. In the configuration categories list, click **Private Networks**.
6. Click the **Add** (green plus symbol) icon.
7. In the Add Private Network panel, add the HQ Network virtual wire as a subnet accessible to SSL VPN-Plus clients.

Option	Action
Network	Type **`192.168.20.0`** in the text box.
Netmask	Type **`255.255.255.0`** in the text box.
Description	Leave blank.
Send Traffic	Leave the **Over Tunnel** radio button selected.
Enable TCP Optimization	Leave the check box selected.
Ports	Leave blank.
Status	Leave the **Enabled** radio button selected.

8. Click **OK**.

Task 6: Create and Install an Installation Package

Installation packages are presented to users when logged in to the SSL VPN-Plus Web portal.

Student A performs this task. Student B verifies the settings.

1. In the configuration categories list, click **Installation Package**.
2. Click the **Add** (green plus symbol) icon.
3. In the Add Installation Package panel, configure a basic installation package.

Option	Action
Profile Name	Type **`Basic Installation Package`** in the text box.
Gateway	Type **`172.20.11.11`** in the text box.
Port	Leave the default of `443`, and click **OK**.
Create installation package for	Leave the **Windows** check box selected.
Description	Leave blank.
Status	Leave the **Enabled** radio button selected.
Installation Parameters for Windows	Select the following check boxes. • Allow remember password • Enable silent mode installation • Create desktop icon

4. Click **OK** and wait for the update to complete.
5. In the Firefox window, open a new browser tab.
6. Click the **SSL VPN-Plus** favorite link.
7. When prompted, log in by using the VPN user credentials.
   - Username: `vpnuser`
   - Password: `vmware1!`

8. Verify that the following tabs appear in the upper-left corner of the SSL VPN-Plus Web portal under the branding graphic.
   - Full Access
   - Tools
9. On the Full Access tab, click the **Basic Installation Package** link.

   A new browser window opens.
10. Click the **Please click here to start the installation** link.
11. When prompted, click **Save File**.
12. When the download completes, close the installation browser window.
13. Minimize the Firefox window.
14. On your workspace desktop, double-click the VMware_index.html-Setup.exe icon.
15. When prompted, click **Run**.
16. Restore the Firefox window.
17. In the SSL VPN-Plus portal, click the **Logout** link.
18. When prompted, click **OK**.
19. Close the SSL VPN-Plus tab.

Task 7: Test Network Access by Using the SSL VPN-Plus Client Application

When the SSL VPN-Plus client connects, an IP address assignment occurs and the client receives a list of subnets accessible through the tunnel. Student B performs this task. Student A verifies the settings.

1. Minimize the Firefox window.
2. On the lab desktop, double-click the **Network Connections** shortcut.
3. Verify that a disconnected network adapter named `Local Area Connection` is present in the network adapters list and that the description begins with VMware SSL VPN-Plus Client.
4. Close the Network Connections window.
5. On your lab desktop, double-click the **VMware Tray** shortcut.

   The VMware Tray shortcut launches the SSL VPN-Plus client application.
6. In the SSL VPN-Plus Client - Login window, click **Login**.

7. When prompted to log in, perform the following actions.

   a. Type **`vpnuser`** in the **User Name** text box.

   b. Type **`vmware1!`** in the **Password** text box.

   c. Select the **Remember password** check box.

   d. Click **OK**.

8. Click **OK** to dismiss the connection established message.

9. In the Windows system tray, on the right side of the task bar, right-click the SSL VPN-Plus Client icon and select **Statistics** > **Connection Information**.

10. In the SSL VPN-Plus Client - Statistics window, click the **Advanced** tab and verify the following.

    - The Gateway IP address and port is `172.20.11.11:443`.
    - The Tunnel mode is `Split Tunnel`.
    - The private subnets are `192.168.20.0/255.255.255.0`.
    - No subnets have been excluded.
    - The Virtual IP assigned to the adapter is in the range `192.168.200.2 - 192.168.200.254`.

11. Close the SSL VPN-Plus Client - Statistics window.

12. Restore the Firefox window.

13. Open a new browser tab and browse the following URL.

    `http://192.168.20.10`

14. Verify that the Web page reports the same IP address as browsed.

15. In the Windows tray, right-click the **SSL VPN-Plus Client** icon and select **Exit**.

16. When prompted, click **Yes**.

17. In the Firefox window, with the index tab selected, click the page refresh icon.

18. Verify that the Web page can no longer be loaded.

19. Close the browser tab.

20. In the vShield Manager interface, click the **blue back-arrow** button.

Lab 11

Configuring vShield Edge Load Balancing

Objective: Configure load balancing to distribute HTTP load among two or more Web servers

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Add an External Interface IP for Load-Balancing Use
3. Configure a Load-Balancing Pool
4. Configure a Load-Balancing Virtual Server
5. Test Round-Robin Load Balancing

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing class from the previous lab, skip to the next task.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the vSphere administrator, using the standard lab password.
4. In the vSphere Web Client interface, navigate to **vCenter > Hosts and Clusters**.
5. Power on the following virtual machines.
   - Branch > Branch Application > Web4
   - Branch > Branch Application > Web5
   - HQ > HQ Application > Web1
   - HQ > HQ Application > Web3
6. In the Firefox window, open a new browser tab.
7. Click the **vShield Manager** favorite link.
8. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.
9. In the left pane, expand the **Datacenters** container and select **Datacenter-A**.
10. In the right pane, click the **Network Virtualization** tab.

Task 2: Add an External Interface IP for Load-Balancing Use

Student A performs this task. Student B verifies the settings.

1. In the edge list, select the **HQ-Edge** item.
2. Click the **Actions** menu and select **Manage**.
3. Click the **HQ-Edge > Configure** button.
4. In the interface list, select the **External** interface item.
5. Click the **Edit** (pencil) icon.

6. In the **Edit Edge Interface** panel, perform the following actions.
   a. Under Configure Subnets, select the existing row.
   b. Click the **Edit** (pencil) icon.
   c. In the Edit Subnet panel, click the **Add** (green plus symbol) icon to add the IP address to be used by the load-balancing virtual server.

Option	Action
IP Address	Type **`172.20.11.13`** in the IP Address text box and click **OK**.

   d. Click **Save** to close the Edit Subnet panel.
   e. Click **Save** to close the Edit Edge Interface panel.

Task 3: Configure a Load-Balancing Pool

A load balancing pool identifies the hosts and the services to be associated with a virtual server.

Student B performs this task. Student A verifies the settings.

1. Click the **HQ-Edge > Load Balancer** button.
2. Verify that the Pools link is selected.
3. Click the **Add** (green plus symbol) icon.
4. In the Add Pool panel, perform the following actions.
   a. Type **`WebPool`** in the **Name** text box, and click **Next**.
   b. Under Services, configure HTTP load-balancing parameters.

Option	Action
HTTP Service	Select the **HTTP Enabled** check box.
HTTP Balancing Method	Leave **ROUND_ROBIN** selected.
HTTP Port	Leave the default of `80`.

   c. Click **Next**.
   d. Under Health Check, click **Next** to accept all default configuration values.

e. Under Members, click the **Add** (green plus symbol) icon.

f. In the Add member panel, add the Web1 server IP address to the round-robin pool.

Option	Action
IP Address	Type **`192.168.20.10`** in the text box. This is the Web1 IP address on the HQ Network virtual wire.
Weight	Leave the default of `1`.
HTTP Port	Leave the default of `80`.
HTTP Monitor Port	Leave the default of `80`.

g. Click the **Add** button.

h. Click the **Add** (green plus symbol) icon to add a second member.

i. In the Add member panel, add the Web2 server IP address to the round-robin pool.

Option	Action
IP Address	Type **`192.168.20.11`** in the text box. This is the Web2 IP address on the HQ Network virtual wire.
Weight	Type **`2`** in the text box.
HTTP Port	Leave the default of `80`.
HTTP Monitor Port	Leave the default of `80`.

j. Click the **Add** button.

k. Click **Next**.

l. Under Ready To Complete, click **Finish**.

5. Click the **Enable** button to enable the Load Balancer service.

6. Click the **Publish Changes** button located near the upper-right corner of the page, in the green bar.

Task 4: Configure a Load-Balancing Virtual Server

A virtual server provides a single point of access to pool hosts. In this lab, you configure the virtual server without persistence so that basic round-robin operations can be more readily observed.

Student A performs this task. Student B verifies the settings.

1. Click the **Load Balancer** > **Virtual Servers** link.
2. Click the **Add** (green plus symbol) icon.
3. In the Add Virtual Server panel, configure the load-balancing virtual server parameters.

Option	Action
Name	Type **`VirtualServer`** in the text box.
Description	Leave blank.
IP Address	Type **`172.20.11.13`** in the text box.
Existing Pool	Leave **WebPool** selected.
HTTP Service	Select the **Enable** check box.
HTTP Persistence Method	Select **None** from the drop-down menu.
Enabled	Leave the check box selected.
Enable logging	Select the check box.

4. Click the **Add** button.
5. Click the **Publish Changes** button, located near the upper-right corner of the page, in the green bar.

Task 5: Test Round-Robin Load Balancing

Student B performs this task. Student A verifies the settings.

1. In the Firefox window, click the **vSphere Web Client** tab.
2. In the Hosts and Clusters inventory pane, select the **HQ** > **HQ Application** > **Web2** virtual machine item.
3. In the center pane, select **Power On** from the **Actions** drop-down menu, and wait for the operation to complete.

4. In the center pane, select **Open Consol**e from the **Actions** drop-down menu.
5. Monitor the virtual machine startup. When you are prompted to log in, close the Web2 browser tab.
6. In the Firefox window, open a new browser tab.
7. Click the **Round Robin** favorite link.
8. After the Web1 Web page is displayed, perform the following actions to verify round-robin operation.
    a. In the Firefox window, click the page refresh icon, located to the right of the URL text box.
    b. Note the server IP address presented by the Web page.
    c. Repeat steps a and b several times, observing the Web page changes.
9. Close the browser tab.
10. In the vShield Manager interface, click the **blue back-arrow** icon.

Lab 12

Configuring vShield Edge High Availability

Objective: Configure and test vShield Edge high availability

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Configure High Availability
3. Examine the High Availability Service Status and Monitor Heartbeat Operations
4. Trigger Failover
5. Restore a Powered-Off Node

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing class from the previous lab, skip to the next task.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface, as the vSphere administrator, using the standard lab password.
4. In the vSphere Web Client interface, navigate to **vCenter > Hosts and Clusters**.
5. Power on the following virtual machines.
    - Branch > Branch Application > Web4
    - Branch > Branch Application > Web5
    - HQ > HQ Application > Web1
    - HQ > HQ Application > Web2
    - HQ > HQ Application > Web3
6. In the Firefox window, open a new browser tab.
7. Click the **vShield Manager** favorite link.
8. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.
9. In the left pane, expand the **Datacenters** container and select **Datacenter-A**.
10. In the right pane, click the **Network Virtualization** tab.

Task 2: Configure High Availability

When high availability is configured and enabled, a second VMware® vShield Edge™ is deployed, in standby mode.

Student A performs this task. Student B verifies the settings.

1. In the edge list, select the **HQ-Edge** item.
2. Click the **Actions** menu and select **Manage**.

3. In the Settings page, locate the **HA Configuration** section.
4. Click the HA Configuration **Change** link.
5. In the Change HQ Configuration panel, configure high-availability options for the HQ-Edge.

Option	Action
HQ Status	Select the **Enable** radio button.
vNIC	Select **Shared Network** from the drop-down menu.
Declare Dead Time	Leave the default of `6`.
Management IPs	Type the following CIDR format IP addresses in the provided text boxes. • **`192.168.222.1/30`** • **`192.168.222.2/30`**

6. Click **OK**.
7. At the top of the Settings page, monitor the current job status to completion.
8. When the current job completes, scroll down to the deployed appliance list at the bottom of the page.

   A second appliance, named HQ-Edge-1, has been deployed.
9. If the HQ-Edge-1 appliance status is `Undeployed`, perform the following actions.
   a. In the upper-right corner of the page, click the **Refresh** link.
   b. In the edge list, select the **HQ-Edge** item.
   c. Select the **Actions** menu and select **Manage**.
   d. Scroll down to the bottom of the page, and verify that the HQ-Edge-1 appliance status is `Deployed`.
10. At the top of the page, click the **General** tab.
11. In the right pane, verify that a single-service virtual machine has been deployed to each ESXi host.

    When high availability is enabled, the secondary edge appliance is automatically deployed to a different ESXi host than the primary appliance.
12. In the Firefox window, click the **vSphere Web Client** tab.

13. Click the refresh icon, located to the left of the logged-in user name.

14. In the Hosts and Clusters inventory pane, verify that the following edge appliances appear in the **HQ** > **HQ Infrastructure** pool.

    - `HQ-Edge-0`
    - `HQ-Edge-1`

Task 3: Examine the High Availability Service Status and Monitor Heartbeat Operations

When HA is enabled, the active and passive nodes send heartbeat information across the specified virtual wire. The heartbeat traffic and high-availability status can be viewed by logging in to the active node and executing the appropriate CLI commands.

Student A and student B perform this task.

Use the following information from the class configuration handout:

- vShield Manager default administrator user name __________________________
- Standard lab password __________________________

1. Minimize the Firefox window.
2. On the lab desktop, double-click the **Putty** shortcut.
3. In the PuTTY window, double-click the **HQ - Edge** saved profile.
4. Click **Yes** to confirm the PuTTY security alert.
5. When prompted, log in as the default vShield manager administrator, using the standard lab password.
6. Show the high-availability service status by executing the following command.

   ```
   show service highavailability
   ```

7. Use the command output to verify the following.

   a. The status is `running`.

   b. The Unit name is `vshield-edge-1-0`.

   c. The Unit State is `active`.

   d. The Interface(s) list includes `vNic_1`.

   e. The Peer host is `vshield-edge-1-1`.

8. Show heartbeat traffic by executing the following command.

   ```
   debug packet display interface vNic_1
   ```

9. Allow the command to run for a few seconds and then press Ctrl+C.
10. In the command output, verify that communication is occurring between the following two IP addresses.
    a. `192.168.222.1`
    b. `192.168.222.2`

    NOTE

    The heartbeat traffic uses a /30 network that is overlaid onto the selected virtual wire. In this case, the selected virtual wire subnet is 192.168.1.0/24 (Shared Network), and the heartbeat traffic is using a 192.168.222.0/30 network.

Task 4: Trigger Failover

If the active node fails for any reason, the inactive node quickly assumeS the active role.

Student A and student B perform this task. Student A shuts down the vShield Edge appliance.

1. Leave the PuTTY window open.
2. Restore the Firefox window.
3. In the vSphere Web Client Hosts and Clusters inventory, select the **HQ > HQ Infrastructure > HQ-Edge-0** item.
4. In the middle panel, select **Shut Down Guest OS** from the **Actions** menu.
5. When prompted, click **Yes** to confirm the shut down.
6. Minimize the Firefox browser window.
7. Click **OK** to dismiss the PuTTY Fatal Error dialog box.
8. Close the PuTTY window.
9. On the lab desktop, double-click the **Putty** shortcut.
10. In the PuTTY window, double-click the **HQ - Edge** saved profile.
11. When prompted, log in as the default vShield manager administrator, using the standard lab password.
12. Show the high availability service status by executing the following command.

    ```
    show service highavailability
    ```
13. Use the command output to verify the following.
    a. The status is `running`.
    b. The Unit name is `vshield-edge-1-1`.

c. The Unit State is `active`.

d. The Interface(s) list includes `vNic_1`.

e. The Peer host is `vshield-edge-1-0`, which has a status of unreachable.

14. Show heartbeat traffic by executing the following command and allowing it to continuously run.

```
debug packet display interface vNic_1
```

15. Without stopping the command, verify that the `192.168.222.2` host is attempting to communicate with the `192.168.222.1` host, but is receiving no replies.

16. Leave the debug command running and restore the Firefox window.

Task 5: Restore a Powered-Off Node

When a failed node is returned to service, the node automatically assumes the secondary or passive role.

Student A and Student B perform this task. Student A powers on the vShield Edge appliance.

1. In the Hosts and Clusters inventory panel, select the **HQ** > **HQ Infrastructure** > **HQ-Edge-0** virtual machine item.
2. In the middle pane, select **Power On** from the **Actions** drop-down menu.
3. Minimize the Firefox window.
4. Monitor the debug command output in Putty until bidirectional communication between the two vShield Edge appliances is observed.
5. Press Ctrl+C to stop the debug command.
6. Show the high-availability service status by executing the following command.

```
show service highavailability
```

7. Use the command output to verify the following.

   a. The status is `running`.

   b. The Unit name is `vshield-edge-1-1`.

   c. The Unit State is `active`.

   d. The Interface(s) list includes `vNic_1`.

   e. The Peer host is `vshield-edge-1-0`, which has a status of good.

8. Close the PuTTY window.
9. When prompted, click **OK**.

10. Restore the Firefox window and click the **vShield Manager** tab.

11. In the right pane, click the **Network Virtualization** tab.

Lab 13

Installing and Configuring vShield App

Objective: Install and configure vShield App on each ESXi host

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Install vShield App for Each ESXi Host
3. Examine Changes in the vShield Manager and vSphere Web Client Interfaces
4. Configure vShield App to Send Events to a Syslog Server
5. Change vShield App Fail-Safe Behavior

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing class from the previous lab, skip to the next task.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the vSphere administrator, using the standard lab password.
4. In the vSphere Web Client interface, navigate to **vCenter > Hosts and Clusters**.
5. Power on the following virtual machines.
   - Branch > Branch Application > Web4
   - Branch > Branch Application > Web5
   - HQ > HQ Application > Web1
   - HQ > HQ Application > Web2
   - HQ > HQ Application > Web3
6. In the Firefox window, open a new browser tab.
7. Click the **vShield Manager** favorite link.
8. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.
9. In the left pane, expand the **Datacenters** container and select **Datacenter-A**.

Task 2: Install vShield App for Each ESXi Host

VMware® vShield App™ is installed separately for each VMware ESXi™ host.

Student A performs this task. Student B verifies the settings.

1. In the vShield Manager inventory panel, expand the following containers.
   a. Datacenters > Datacenter-A > Branch
   b. Datacenters > Datacenter-A > HQ
2. Select the **HQ > esxi-01a.vclass.local** host item and wait for the summary tab to update.

3. In the right pane, on the Summary tab, click the vShield App **Install** link.
4. Configure the following vShield App installation settings.

Option	Action
Datastore	Select **Shared-Datastore** from the drop-down menu.
Management Port Group	Select **pg-HQ-Externa**l from the drop-down menu.
vShield App IP Address	Type **`172.20.11.200`** in the text box.
Netmask	Type **`255.255.255.0`** in the text box.
Default Gateway	Type **`172.20.11.10`** in the text box.
vShield Endpoint	Leave the check box deselected.

5. In the upper-right corner of the Summary page, click the **Install** button.
6. Monitor the installation process through all three phases to completion.

   The installation takes a few minutes to complete.
7. In the vShield Manager inventory pane, select the **HQ** > **esxi-01b.vclass.local** host item.
8. In the right pane, on the Summary tab, click the vShield App **Install** link.
9. Configure the following vShield App installation settings.

Option	Action
Datastore	Select **Shared-Datastore** from the drop-down menu.
Management Port Group	Select **pg-HQ-Externa**l from the drop-down menu.
vShield App IP Address	Type **`172.20.11.201`** in the text box.
Netmask	Type **`255.255.255.0`** in the text box.
Default Gateway	Type **`172.20.11.10`** in the text box.
vShield Endpoint	Leave the check box deselected.

10. In the upper-right corner of the Summary page, click the **Install** button.

11. Monitor the installation process through all three phases to completion.
12. In the vShield Manager inventory pane, select the **Branch** > **esxi-02a.vclass.local** host item.
13. In the right pane, on the Summary tab, click the vShield App **Install** link.
14. Configure the following vShield App installation settings.

Option	Action
Datastore	Select **Shared-Datastore** from the drop-down menu.
Management Port Group	Select **pg-Branch-External** from the drop-down menu.
vShield App IP Address	Type **`172.20.110.200`** in the text box.
Netmask	Type **`255.255.255.0`** in the text box.
Default Gateway	Type **`172.20.110.10`** in the text box.
vShield Endpoint	Leave the check box deselected.

15. In the upper-right corner of the Summary view, click the **Install** button.
16. Monitor the installation process through all three phases to completion.

Task 3: Examine Changes in the vShield Manager and vSphere Web Client Interfaces

Student B performs this task. Student A verifies the settings.

1. In the vShield Manager inventory, expand the **Branch** > **Branch Application** resource pool.
2. Select the **Web4** virtual machine item.
3. In the right pane, on the Summary tab, verify the following services hierarchy.
   - `vShield-FW-esxi-02a.vclass.local`
     - `Web4 (192.168.1.200)`
4. In the vShield Manager inventory, expand the **HQ** > **HQ Application** resource pool.
5. Select the **Web1** virtual machine item.
6. In the right pane, on the Summary tab, verify the following services hierarchy.
   - `vShield-FW-esxi-01a/b.vclass.local`
     - `Web1 (192.168.20.10)`

7. Expand the **Web1** virtual machine item and select **Network Adapter 1**.
8. In the right pane, locate the Connected vSwitches and vShields section.
9. Verify for each host that the path is through a vShield-FW appliance.
10. In the Firefox window, click the **vSphere Web Client** tab.
11. At the top of the left pane, click the **Networking** icon.
12. Click the refresh icon located at the top of the page and to the left of the logged-in user name.
13. In the left pane, verify that a new standard switch network named `vmservice-vshield-pg` is listed.
14. At the top of the left pane, click the **Hosts and Clusters** icon.
15. In the Hosts and Clusters inventory pane, verify that the following virtual machines are listed at the Branch cluster level.
    - `vShield-FW-esxi-02a.vclass.local`
16. Verify that the following virtual machines are listed at the HQ cluster level.
    - `vShield-FW-esxi-01a.vclass.local`
    - `vShield-FW-esxi-01b.vclass.local`
17. In the inventory panel, select the **Branch** > **vShield-FW-esxi-02a.vclass.local** virtual machine item.
18. In the right pane, on the Summary tab, use the VM Hardware section to verify the following hardware characteristics.
    - CPU(s): `2`
    - Memory: `1024 MB`
    - Hard disk: `5.00 GB`
    - Network adapter 1: Connects to the `pg-Branch-External` port group.
    - Network adapter 2 and 3: Connect to port groups created by vCloud Networking and Security.

Task 4: Configure vShield App to Send Events to a Syslog Server

Each vShield App instance can be configured to send log information to one or more syslog servers.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- Syslog server address ____________________________

1. In the Firefox window, click the **vShield Manager** tab.
2. In the vShield Manager inventory, select the **HQ > esxi-01a.vclass.local** host item.
3. In the right pane, on the Summary tab, locate the **Service Virtual Machines** section.
4. Expand the **vShield-FW-esxi-01a.vclass.local (172.20.11.200)** instance.
5. Scroll to the bottom of the form to locate the **Syslog Servers** section.
6. Configure the first syslog server by performing the following actions.
    a. In the **IP Address** text box, type the Syslog server address.
    b. Select **Info** from the **Log Level** drop-down menu.
    c. Click the **Save** button.
7. Scroll to the top of the form, click the **Force Sync** link, and wait for the update to complete.
8. In the vShield Manager inventory, select the **HQ > esxi-01b.vclass.local** host item.
9. In the right pane, on the Summary tab, locate the **Service Virtual Machines** section.
10. Expand the **vShield-FW-esxi-01b.vclass.local (172.20.11.201)** instance.
11. Scroll to the bottom of the form to locate the **Syslog Servers** section.
12. Configure the first syslog server by performing the following actions.
    a. In the **IP Address** text box, type the Syslog server address.
    b. Select **Info** from the **Log Level** drop-down menu.
    c. Click the **Save** button.
13. Scroll to the top of the form, click the **Force Sync** link, and wait for the update to complete.
14. In the vShield Manager inventory, select the **Datacenter-A > Branch > esxi-02a.vclass.local** host item.
15. In the right pane, on the Summary tab, locate the **Service Virtual Machines** section.
16. Expand the **vShield-FW-esxi-02a.vclass.local (172.20.110.200)** instance.
17. Scroll to the bottom of the form to locate the **Syslog Servers** section.
18. Configure the first syslog server by performing the following actions.
    a. In the **IP Address** text box, type the Syslog server address.
    b. Select **Info** from the **Log Level** drop-down menu.
    c. Click the **Save** button.
19. Scroll to the top of the form, click the Force Sync link, and wait for the update to complete.

Task 5: Change vShield App Fail-Safe Behavior

Student B performs this task. Student A verifies the settings.

1. In the left pane, under Settings & Reports, select **vShield App**.
2. In the right pane, in the Fail Safe section, click the **Change** link.
3. When prompted, click **Yes** to change the fail-safe policy to **allow**.

Lab 14

Working with the vShield App Firewall

Objective: Control network traffic by using vShield App firewall rules

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Create a Firewall Rule to Restrict Inbound HTTP Traffic
3. Create a Firewall Rule to Restrict Inbound FTP Traffic

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing class from the previous lab, skip to the next task.

Student B performs this task. Student A verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the vSphere administrator, using the standard lab password.
4. In the vSphere Web Client interface, navigate to **vCenter > Hosts and Clusters**.
5. Power on the following virtual machines.
   - Branch > Branch Application > Web4
   - Branch > Branch Application > Web5
   - HQ > HQ Application > Web1
   - HQ > HQ Application > Web2
   - HQ > HQ Application > Web3
6. In the Firefox window, open a new browser tab.
7. Click the **vShield Manager** favorite link.
8. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.

Task 2: Create a Firewall Rule to Restrict Inbound HTTP Traffic

Create a VMware® vShield App™ firewall rule that restricts inbound HTTP traffic destined for load-balanced servers.

Student B performs this task. Student A verifies the settings.S

1. In the vShield Manager inventory pane, select **Datacenters > Datacenter-A**.
2. In the right pane, click the **Network Virtualization** tab.
3. Click the **Networks** link.
4. In the networks list, click the **HQ Network** link.

5. Click the **HQ Network** > **Security** button.
6. Above the general rules list, click the **Add** (green plus symbol) icon.

   A new rule is added to the list, highlighted in blue.
7. Point to the new rule **Name** cell and click the **plus symbol** icon.
8. In the Rule Name panel, type **`Deny HTTP`** in the text box and click **OK**.
9. Point to the **Destination** cell and click the **plus symbol** icon.
10. In the input panel, perform the following actions.
    a. Select **IP Addresses** from the drop-down menu.
    b. At the bottom of the panel, click the **New IP Addresses** link.
    c. In the Add IP Addresses panel, configure an address set that includes the load-balanced Web servers.

Option	Action
Name	Type **`Round Robin Addresses`** in the text box.
Description	Leave blank.
IP Addresses	Type **`192.168.20.10,192.168.20.11`** in the text box.

    d. Click **OK**.
11. Point to the **Service** cell and click the **plus symbol** icon.
12. In the input panel, perform the following actions.
    a. Sort the Available list by name.
    b. Scroll down and select the **HTTP** service check box.
    c. Click the **blue right-arrow** to move the HTTP service from the Available list to the Selected list.
    d. Click **OK**.
13. Point to the **Action** cell and click the **plus symbol** icon.
14. In the input panel, click **Block** and **Log**.
15. Click **OK**.
16. Click the **Publish Changes** button, located above the rules list, in the green bar.
17. In the Firefox window, open a new browser tab.

18. Click the **Round Robin** link.
19. If the Web1 or Web2 web page is displayed, wait 10 seconds and click the page refresh button.
20. Verify that a `503 Service Unavailable` message is displayed.
21. In the Firefox window, click the **vShield Manager** tab.
22. In the **`Deny HTTP`** rule, point to the **Destination** cell and click the **plus symbol** icon.
23. In the lower-left corner of the destination panel, expand **Advance options**.
24. Select the **Negate Destination** check box and click **OK**.
25. Click the **Publish Changes** button.
26. In the Firefox window, click the http://**172.20.11.13/** tab.
27. Click the page refresh button.
28. If a 503 error message appears, wait 10 seconds and click the page refresh button.
29. When either the Web1 or Web2 web page is displayed, close the browser tab.

    With the destination negated, the firewall rule is now blocking HTTP traffic to all hosts on the HQ Network except the round-robin web servers.
30. In the vShield Manager interface, under the **Network Virtualization** tab, click the **Refresh** link.

Task 3: Create a Firewall Rule to Restrict Inbound FTP Traffic

Create a vShield App firewall rule that restricts inbound FTP traffic destined to a virtual wire that spans multiple clusters.

Student A and Student B perform this task. Student A powers on the vShield Edge appliance.

1. In the Firefox window, open a new browser tab and navigate to the following URL.

   ftp://192.168.1.200
2. After the FTP server index page is displayed, click the **vShield Manager** tab.
3. In the network list, click the **Shared Network** link.
4. Click the **Shared Network > Security** button.
5. In the general rules list, select the **Default Rule** row.
6. Point to the **Action** cell and click the **plus symbol** icon.
7. In the input panel, select the **Log** radio button.
8. Click **OK**.
9. Above the general rules list, click the **Add** (green plus symbol) icon.
10. Point to the new rule **Name** cell and click the **plus symbol** icon.

11. In the Rule Name panel, type `Deny FTP` in the text box and click **OK**.
12. Point to the **Source** cell and click the **plus symbol** icon.
13. In the input panel, perform the following actions.
    a. In the Available list, select the **Shared Network** check box.
    b. Click the **blue right-arrow** button.
    c. In the lower-left corner of the panel, expand **Advance** options.
    d. Select the **Negate Source** check box.
    e. Click **OK**.
14. Point to the **Destination** cell and click the **plus symbol** icon.
15. In the input panel, perform the following actions.
    a. In the Available list, select the **Shared Network** check box.
    b. Click the **blue right-arrow** button.
    c. Click **OK**.
16. Point to the **Service** cell and click the **plus symbol** icon.
17. In the input panel, perform the following actions.
    a. Sort the Available list by name.
    b. Scroll down and select the **FTP** service check box.
    c. Click the **blue right-arrow** button.
    d. Click **OK**.
18. Point to the **Action** cell and click the **plus symbol** icon.
19. In the input panel, click the **Block** and **Log** radio buttons.
20. Click **OK**.
21. Click the **Publish Changes** button.
22. In the Firefox window, click the **Index of ftp://192.168.1.200/** tab.
23. Click the page refresh button and verify that the FTP index cannot be loaded.
24. In the same browser tab, verify HTTP connectivity by browsing to the following URL.

    `http://192.168.1.200`
25. After the Web4 web page appears, close the browser tab.
26. In the Firefox window, click the vSphere Web Client tab.

27. In the Hosts and Clusters inventory panel, select the **HQ > HQ Application > Web3** virtual machine item.

28. In the right pane, select **Open Console** from the **Actions** drop-down menu.

29. If prompted to log in, perform the following actions.

    a. In the upper-right corner of the page, click the **Send Ctrl-Alt-Delete** button.

    b. Log in as the client administrator, using the standard lab password.

30. On the client desktop, double-click the **Internet Explorer** shortcut.

31. In the Internet Explorer window, navigate to the following URL.

    ```
    ftp://192.168.1.200
    ```

    NOTE

    The Web4 FTP file list is displayed. The firewall rule added in the preceding task denied FTP traffic originating from any source other than the HQ Network because the source was negated.

32. In the Firefox window, click the **vShield Manager** tab.

33. In the firewall rule list, point to the Deny FTP rule **Source** cell and click the **plus symbol** icon.

34. In the input panel, select the **Shared Network** check box and click the **blue left-arrow** icon.

35. Click **OK**.

36. Click the **Publish Changes** button.

37. In the Firefox window, click the **Web3** tab.

38. In the Internet Explorer window, click the page refresh or **Go** button.

39. When prompted, click **OK** to dismiss the FTP Folder Error dialog box.

    NOTE

    The firewall rule now blocks FTP traffic originating from all sources, including hosts on the same broadcast domain as the FTP server.

40. In the Internet Explorer window, verify HTTP connectivity by navigating to the following URL.

    ```
    http://192.168.1.200
    ```

41. Close the Internet Explorer window.

42. In the Firefox window, close the **Web3** browser tab.

43. Click the **vShield Manager** tab.

44. In the upper-right corner of the page, under the Network Virtualization tab, click the **Refresh** link.

Lab 15

Using Flow Monitoring

Objective: Examine flow statistics and define a firewall rule from a flow

In this lab, you will perform the following tasks:

1. Prepare for the Lab
2. Examine Flow-Monitoring Statistics
3. Add a Firewall Rule Based on an Allowed Flow
4. Verify That the Firewall Rule Is in Effect

Work in teams of two students. Each task identifies student A or student B as being responsible for performing the task, with the other student being responsible for verifying the settings.

Task 1: Prepare for the Lab

If you are continuing class from the previous lab, skip to the next task.

Student A performs this task. Student B verifies the settings.

Use the following information from the class configuration handout:

- VMware vSphere® administrator user name ________________________
- Standard lab password ________________________

1. On the lab desktop, double-click the **Firefox** browser shortcut.
2. Click the **vSphere Web Client** favorite link.
3. Log in to the VMware vSphere® Web Client interface as the vSphere administrator, using the standard lab password.
4. In the vSphere Web Client interface, navigate to **vCenter > Hosts and Clusters**.
5. Power on the following virtual machines.
    - Branch > Branch Application > Web4
    - Branch > Branch Application > Web5
    - HQ > HQ Application > Web1
    - HQ > HQ Application > Web2
    - HQ > HQ Application > Web3
6. In the Firefox window, open a new browser tab.
7. Click the **vShield Manager** favorite link.
8. Log in to the VMware® vShield Manager™ interface as the vSphere administrator, using the standard lab password.
9. In the left pane, expand the **Datacenters** container and select **Datacenter-A**.
10. In the right pane, click the **Network Virtualization** link.
11. Click the **Networks** link.

Task 2: Examine Flow-Monitoring Statistics

Examine the statistics for the Top Flows, Top Destinations, and Top Sources categories.

Student A performs this task. Student B verifies the settings.

1. In the networks list, click the **Shared Network** link.
2. Click the **Shared Network > Flow Monitoring** button.

3. Verify that the **Flow Monitoring** > **Summary** link is selected.
4. On the far right side of the page, across from the Summary and Details links, click the Time Interval **Change** link.
5. In the interval panel, select the **Last 1 week** radio button and click **Update**.
6. Verify that the **Top Flows** button is selected.
7. Use the Top Flows table to determine the following.
    a. Which flow has the highest volume of bytes
    b. Which flow has the highest volume of packets
8. Use the mouse wheel or the vertical scroll bar to view the graph.
9. Point to the apex of three different-colored lines and determine which network protocol is reported.
10. Scroll to the top of the form and click the **Top Destinations** button.
11. Use the Top Destinations table to determine the following.
    a. Which destination has the highest volume of incoming bytes
    b. Which destination has the highest volume of packets
12. Use the mouse wheel or the vertical scroll bar to view the graph.
13. Point to the apex of two different-colored lines to determine which destination is reported.
14. Scroll to the top of the form and click the **Top Sources** button.
15. Use the Top Sources table to determine the following.
    a. Which source has the highest volume of bytes
    b. Which source has the highest volume of packets
16. Use the mouse wheel or the vertical scroll bar to view the graph.
17. Point to the apex of two different-colored lines to determine which source is reported.

Task 3: Add a Firewall Rule Based on an Allowed Flow

New firewall rules can be configured by using the details view of a blocked or allowed flow.

Student B performs this task. Student A verifies the settings.

1. Scroll to the top of the Flow Monitoring page and click the **Details** link.
2. Verify that the **Allowed Flows** button is selected.
3. In the allowed flows table, click the **Oracle HTTP Server listen port** link.

4. Select a transaction with a source of `Web3 (192.168.1.100)` and a destination of `Web4 (192.168.1.200)`.
5. Use the horizontal scroll bars to view the Actions cell.

   One or more horizontal scroll bars might be shown at the bottom of the page. Move each slider to the far-right position.
6. For the selected transaction, click the **Add Rule** link.
7. In the Add Rule panel, configure a firewall rule that blocks HTTP requests between the Web3 and Web4 virtual machines.

Option	Action
Name	Type **`Block Web3 to Web4 HTTP`** in the text box.
Source	a. Click the **plus symbol** icon. b. Click the **New IP Addresses** link. c. In the Name text box, type **`Web3 IP Address`**. d. Click **OK**.
Destination	e. Click the **plus symbol** icon. f. Click the **New IP Addresses** link. g. In the Name text box, type **`Web4 IP Address`**. h. Click **OK**.
Service	Cannot be modified
Action	Select the **Block** radio button.
Enabled	Leave the **Yes** radio button selected.
Logging	Select the **Log** radio button.

8. Click **OK**.
9. At the top of the page, click the **Shared Network > Security** button.
10. Verify that the new rule appears in the general rules list.

Task 4: Verify That the Firewall Rule Is in Effect

New firewall rules can be configured by using the details view of a blocked or allowed flow.

Student A performs this task. Student B verifies the settings.

1. In the Firefox window, select the **vSphere Web Client** tab.
2. In the Hosts and Clusters inventory panel, select the **HQ** > **HQ Application** > **Web3** virtual machine item.
3. In the right pane, select **Open Console** from the **Actions** drop-down menu.
4. If prompted to log in, perform the following actions.
   a. In the upper-right corner of the page, click the **Send Ctrl-Alt-Delete** button.
   b. Log in as the client administrator, using the standard lab password.
5. On the client desktop, double-click the **Internet Explorer** shortcut.
6. In the Internet Explorer window, navigate to the following URL.

   ```
   http://192.168.1.200
   ```

7. Verify that the Web page cannot be displayed.

   NOTE

   In the previous lab, FTP traffic between hosts on the Shared Network virtual wire was blocked by a firewall rule, but HTTP communication was allowed.

8. Close the Internet Explorer window.
9. In the Firefox window, close the **Web3** browser tab.