# Lab: Deploying network workloads

## Scenario

The employees in the IT department at Contoso need to be able to access server systems outside of business hours to correct issues that arise during weekends or holidays. Some of the employees are using computers that aren't members of the contoso.com domain. Other users are running non-Windows operating systems on their computers. To enable remote access for these users, you will provide remote access to Windows Admin Center and secure it with Web Application Proxy and deploy a secure VPN solution using the SSTP VPN protocol.

You are a web server administrator for Contoso and your company is preparing to deploy a new intranet web application on an internal web server. You need to verify the server configuration and install IIS. The website must be accessible using a friendly DNS name and all web connections to and from the server must be encrypted.

## Objectives

After completing this lab, you’ll be able to:

* Deploy and configure Web Application Proxy
* Implement a VPN (virtual private network) solution
* Deploy and configure a web server

## Lab setup

**Estimated time:** 60 minutes

For this lab, you will use the following virtual machines:

* **WS-011T00A-SEA-DC1**
* **WS-011T00A-SEA-ADM1**
* **WS-011T00A-SEA-SVR1**
* **WS-011T00A-SEA-SVR3**
* **WS-011T00A-SEA-CL1**

Sign in by using the following credentials:

* User Name: \*\*Contoso\*
* Password: **Pa55w.rd**

## Exercise 1: Implementing Web Application Proxy

Contoso has decided to make Windows Admin Center available remotely to administrators. To secure Windows Admin Center, you need to deploy Web Application Proxy. For initial testing, you will use pass-through preauthentication. AD FS is being installed on **SEA-SVR1** and Web Application Proxy is being installed on **SEA-SVR3**. Certificates are already installed on both servers in preparation for the installation.

The main tasks for this exercise are as follows:

1. Install AD FS on **SEA-SVR1**.
2. Create DNS entries for AD FS and Web Application Proxy.
3. Install Remote Access management tools.
4. Install Web Application Proxy.
5. Configure Web Application Proxy.
6. Configure a web application.
7. Configure Windows Defender Firewall to allow remote access
8. Test the web application.

### Task 1: Install AD FS on SEA-SVR1

1. On **SEA-SVR1**, at the command prompt, run **powershell.exe**.
2. At the Windows PowerShell prompt, run **C:03.ps1**.

### Task 2: Create DNS entries for AD FS and Web Application proxy

1. On **SEA-ADM1**, in Windows Admin Center, connect to **SEA-DC1**.
2. Use DNS to create two new host records in **Contoso.com**:
   * **remoteapp** resolves to: **172.16.10.14 (SEA-SVR3)**.
   * **fs** resolves to: **172.16.10.12 (SEA-SVR1)**.

### Task 3: Install Remote Access management tools

1. On **SEA-ADM1**, in **Windows Admin Center**, connect to **SEA-ADM1**.
2. Use **Roles and features** to install **Remote Access Management Tools** in Remote Server Administration Tools.

### Task 4: Install Web Application Proxy

1. On **SEA-ADM1**, in **Windows Admin Center**, connect to **SEA-SVR3**.
2. Use **Roles & features** to install the **Web Application Proxy** role service in the **Remote Access** role.

### Task 5: Configure Web Application Proxy

1. On **SEA-ADM1**, in **Server Manager**, open **Remote Access Management**.
2. In **Remote Access Management Console**, use the **Manage a Remote Server** option to connect to **SEA-SVR3**.
3. Use the **Web Application Proxy Wizard** to configure **Web Application Proxy** with following settings:
   * Federation service name: **fs.Contoso.com**
   * User name: \*\*Contoso\*
   * Password: **Pa55w.rd**
   * Certificate: **fs.contoso.com**

**Note:** If you get an error in **Remote Access Management Console** indicating that cmdlets are not found, restart **Remote Access Management Console**.

### Task 6: Configure a web application

1. On **SEA-ADM1**, in **Remote Access Management Console**, publish a web application with the following settings:
   * Pre-authentication: **Pass-through**
   * Name: **RemoteApp**
   * External URL: **https://remoteapp.contoso.com**
   * External certificate: **remoteapp.contoso.com**
   * Backend server URL: **https://SEA-ADM1.contoso.com**

**Note:** You will receive a warning that the external URL and backend URL are different. You can ignore this warning.

### Task 7: Configure Windows Defender Firewall to allow remote access

1. On **SEA-ADM1**, in **Windows Admin Center**, connect to **SEA-ADM1**.
2. Use **Firewall** to create a new firewall rule with the following settings:
   * Name: **SecureWeb**
   * Direction: **Incoming**
   * Action: **Allowed**
   * Enable firewall rule: **Yes**
   * Protocol: **TCP**
   * Local port: **443**
   * Remote port: **blank**
   * ICMP types: **blank**
   * Profiles: **Select All**

### Task 8: Test the web application

1. On **SEA-CL1**, open **Microsoft Edge** and connect to **https://remoteapp.contoso.com**.
2. In **Microsoft Edge**, sign in as **Contoso\* with the password** Pa55.wrd\*\*.

### Exercise 2: Implementing VPN in Windows Server

### Scenario

The first step to implementing VPN is to verify and configure certificate requirements for a SSTP (Secure Socket Tunneling Protocol) VPN. You then must configure the Remote Access server to provide VPN connectivity, and you also must create a remote access policy to ensure that the clients can connect to the server by using the SSTP VPN protocol.

The main tasks for this exercise are as follows:

1. Configure RRAS service and NPS policies for VPN
2. Configure a client VPN connection
3. Test the VPN connection

#### Task 1: Configure RRAS service and NPS policies for VPN

1. On **SEA-ADM1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter:

Install-WindowsFeature -name RemoteAccess,Routing -IncludeManagementTools

Wait for the command to complete, which should take approximately 1 minute.

##### Request certificate for SEA-ADM1

1. On **SEA-ADM1**, In the PowerShell window, enter the following command, and then select Enter: mmc
2. Add the **Certificates** snap-in for the computer account and local computer.
3. In the **Certificates snap-in** console tree, navigate to \*\*Certificates (local)\*, and then request a new certificate.
4. Under **Request Certificates**, configure the **Contoso Web Server** certificate with the following setting:
   * Subject name: Under **Common name**, enter **vpn.contoso.com**
   * Friendly name: **Contoso VPN**
5. In the Certificates snap-in, expand **Personal** and select **Certificates**, and then, in the **details** pane, verify that a new certificate with the name **vpn.contoso.com** is enrolled with **Intended Purposes** of **Server Authentication**.
6. Close the **Microsoft Management Console (MMC)**. When you receive a prompt to save the settings, select **No**.

##### Change the HTTPS bindings

1. Open the **Internet Information Services (IIS) Manager console**.
2. In **Internet Information Services (IIS) Manager**, navigate to **SEA-ADM1/Sites**, and then select **Default Web site**.
3. Configure site bindings by selecting **Contoso VPN** as SSL Certificate. When prompted, select **Yes**.
4. Close the **Internet Information Services (IIS) Manager** console.

##### Configure and enable VPN configuration

1. On **SEA-ADM1**, open **Routing and Remote Access**.
2. Right-click **SEA-ADM1 (local)** or access the context menu, and then select **Configure and Enable Routing and Remote Access**.
3. On the **Welcome to Routing and Remote Access Server Setup Wizard**, select **Next**.
4. On the **Configuration** page, select **Custom configuration**, and then select **Next**.
5. On the **Custom Configuration** page, select **VPN access** and **LAN routing**, and then select **Next**.
6. On the **Completing the Routing and Remote Access Server Setup Wizard** page, select **Finish**. When prompted, select **Start service**.
7. Expand **SEA-ADM1 (local)**, right-click (or access the context menu) **Ports**, and then select **Properties**.
8. Verify that **128** ports exist for **Wan Miniport (SSTP)**, **Wan Miniport (IKEv2)** and**Wan Miniport (L2TP)**. Modify the number of ports for each type of connection to **5**. Disable the use of **Wan Miniport (PPTP)**.
9. Close the **Ports Properties** dialog box, and when prompted, select **Yes**.
10. Right-click (or access the context menu) **SEA-ADM1 (local)**, and then select **Properties**.
11. On the **General** tab, verify that **IPv4 Remote access server** is selected.
12. On the **Security** tab, select the drop-down arrow next to **Certificate**, and then select **vpn-contoso.com**.
13. Select **Authentication Methods**, and then verify that **EAP** is selected as the authentication protocol.
14. On the **IPv4** tab, verify that the VPN server is configured to assign IPv4 addressing by using **Dynamic Host Configuration Protocol (DHCP)**.
15. To close the **SEA-ADM1 (local) Properties** dialog box, select **OK**, and then, when you receive a prompt, select **Yes**.

##### Configure the Remote Access policies

1. On **SEA-ADM1**, from **Server Manager**, open the **Network Policy Server** console.
2. In the **Network Policy Server** console, in the **navigation** pane, expand **Policies**, and then select **Network Policies**.
3. Create a new network policy by using the **New Network Policy Wizard** with the following settings:
   * Policy name: **Contoso IT VPN**
   * Type of network access server: **Remote Access Server(VPN-Dial up)**
   * Windows Groups: **IT**
   * Specify Access Permission: **Access granted**
   * Configure Authentication Methods:
     + Add **Microsoft Secured password (EAP-MSCHAP v2)**
     + **Add Microsoft: Smart Card or other certificate**
     + Clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box
4. Complete the **New Network Policy Wizard** by accepting the default settings on the other pages.
5. Close all open windows.

#### Task 2: Configure a client VPN connection

1. On **SEA-CL1**, right-click (or access the context menu) **Start**, and then select **Network Connections**.
2. In **Network & Internet**, select **VPN**, and then select **Add a VPN connection**.
3. In the **Add a VPN connection** wizard, use the following values and then select **Save**:
   * VPN provider: **Windows (built-in)**
   * Connection Name: **Contoso VPN**
   * Server name or address: **vpn.contoso.com**
   * VPN type: **Secure Socket Tunneling Protocol (SSTP)**
   * Type of sign-in info: **User name and password**
   * Remember my sign-in info: **Cleared**

#### Task 3: Test the VPN connection

1. In **Network & Internet**, select **Contoso VPN**, and then select **Connect**.
2. In the **Sign in** dialog box, in the **User name** field, enter \*\*contoso\*, in the **Password** field, enter **Pa55w.rd**, and then select **OK**.
3. Verify that you are now connected to the VPN server.

##### Verify connection on client and VPN server

1. On **SEA-CL1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter: Get-NetIPConfiguration
2. Examine the output and verify that **Contoso VPN** is listed next to **InterfaceAlias**. Also verify that the **Contoso VPN** interface has been issued an IP Address. This is the IP address for VPN connection assigned by RRAS.
3. Switch to **SEA-ADM1** and maximize the **Routing and Remote Access** snap-in.
4. In the **Routing and Remote Access** snap-in, select **Remote Access Clients (0)** and verify that **Contoso\* is listed under the** User Name\*\* column. This indicates that the user is connected to the VPN Server.
5. Maximize **Server Manager**, and in the **Tools** menu select **Remote Access Management**.
6. In the **Remote Access Management** Console, select **Remote Client Status** and verify that **CONTOSO\* is listed in the details pane under** Connected Clients**. Notice that the VPN protocol used is displayed under the** Protocol/Tunnel\*\* field as **Sstp**.

**Question:** Why did you disable the PPTP authentication protocol when you configured the ports of the VPN Server?

**Answer:** The PPTP protocol is considered highly insecure and you shouldn't use it at all.

**Results**: After completing this exercise, you should have installed and configured the Remote Access server to successfully provide VPN access.

### Exercise 3: Deploying and configuring web server

### Scenario

In this exercise, you will install the web server role on an internal server. You will then verify the installation of IIS and configure remote management of IIS. You will then add an A record in DNS for the new website and enroll a web server certificate. You will then verify that you can reach the website using the new DNS name and that the connection to the website is encrypted using SSL.

The main tasks for this exercise are as follows:

1. Install the Web Server role
2. Configure Web Server options
3. Create and configure a new site
4. Verify site functionality

#### Task 1: Install the Web Server role

1. On **SEA-SVR1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter: Install-WindowsFeature -name Web-Server -IncludeManagementTools Wait for the command to complete, which should take approximately 1 minute.

##### Verify the Web Server installation

1. On **SEA-SVR1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter:Get-eventLog System -After (Get-Date).AddHours(-1) Verify that no errors display in connection with the installation of IIS.
2. Still in a Windows PowerShell command prompt, enter the following command, and then select Enter:Get-eventLog Application -After (Get-Date).AddHours(-1) Verify that only errors with word **License** display under the **Message** column.

##### Verify that the Windows Firewall rules for HTTP and HTTPS traffic are enabled

1. In a Windows PowerShell command prompt, enter the following command, and then select Enter:Get-NetFirewallProfile -Name Domain | Get-NetFirewallRule | where-Object {$\_.DisplayName -like "World Wide Web\*"}
2. This will return information about two rules: one for HTTP and one for HTTPS. Verify that both rules are enabled and allow inbound traffic.

##### Test the default website

1. Switch to **SEA-ADM1** and open Microsoft Edge. In the address bar, enter **http://SEA-SVR1**
2. Verify that IIS displays the default webpage.
3. In the address bar, enter **http://172.16.10.12**
4. Verify that IIS displays the default webpage.

#### Task 2: Configure Web Server options

##### Configure DNS for the default website

1. On **SEA-ADM1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter:Add-DnsServerResourceRecordA -ComputerName SEA-DC1 -Name "www" -ZoneName "contoso.com" -AllowUpdateAny -IPv4Address "172.16.10.12"
2. In the Windows PowerShell command prompt, enter the following command, and then select Enter:Get-DnsServerResourceRecord -ComputerName SEA-DC1 -ZoneName "contoso.com"
3. Verify in the output that the A record you just created exists in the contoso.com DNS zone.

##### Test the website by using DNS names

1. On **SEA-ADM1**, open Microsoft Edge and in the address bar, enter **http://www.contoso.com**
2. Verify that IIS displays the default webpage.

##### Enable remote management of IIS using IIS Manager

1. On **SEA-SVR1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter:Install-WindowsFeature -Name Web-Mgmt-Service. Wait for the command to complete, which should take approximately 1 minute.
2. On **SEA-SVR1**, in the Windows PowerShell command prompt, enter the following command, and then select Enter:Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\WebManagement\Server' -Name EnableRemoteManagement -Value 1
3. On **SEA-SVR1**, in the Windows PowerShell command prompt, enter the following command, and then select Enter:Restart-Service wmsvc

**Note:** Setting this registry key to 1 will enable remote management of IIS. You must restart the **Web Management Service (wmsvc)** after changing the registry key.

1. Switch to **SEA-ADM1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter:Install-WindowsFeature -Name Web-Mgmt-Console,Web-Scripting-Tools. Wait for the command to complete, which should take approximately 1 minute.

**Note:** The output from this command will return **NoChangeNeeded** under the **Exit Code** column. This is because, you already installed the management tools during exercise 1. This step has been left here intentionally to show the complete process of enabling remote management of IIS.

1. Open **Internet Information Services (IIS) Manager** and display the **Start Page**.
2. On the **Start Page**, under **Connection tasks**, select **Connect to a server**. Use the following information to complete the wizard:
   * Server name: **SEA-SVR1**
   * User name: \*\*contoso\*
   * Password: **Pa55w.rd**
   * Connection name: **SEA-SVR1**
3. When prompted by the **Server Certificate Alert** dialog window, select **Connect**.
4. In the **Connections** pane, select **Start Page**. **Notice Recent connections**, **Connection tasks**, **Online resources**, and **IIS News**.
5. In the **Connections** pane, select **SEA-SVR1 (contoso)**. Notice the icons listed in the **Features View** pane. In the **Actions** pane, notice the list of **Manage Server** actions.
6. In the **Connections** pane, expand **SEA-SVR1 (contoso)**, and then select **Sites**. In the **Features View** pane, notice the **Name** of the listed website and its **Status**.
7. In the **Actions** pane, select **Set Website Defaults**. In the **Website Defaults** dialog box, notice the **Application Pool** setting. Select **Cancel**.
8. Leave **Internet Information Services (IIS) Manager** open.

#### Task 3: Create and configure a new site

##### Create a webpage in the Default Website

1. Switch to **SEA-SVR1**, create, and save a new webpage in **Notepad** using the following information:
   * File name: **Default.htm**
   * Location: \*\*c:\*
   * Content:**<p>Contoso intranet running on SEA-SVR1</p>**
2. In the menu bar, select **File**, and then select **Save As**. In the **Save As** dialog box, select **File name**, and then delete \***.txt**. In the **File** name box, enter **c:.htm**. Select the **Save** button.
3. Close **Notepad**.

##### Request a new Web Server certificate

1. On **SEA-SVR1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter:Get-Certificate -Template ContosoWebServer -DnsName www.contoso.com -CertStoreLocation cert:\LocalMachine\My.
2. Wait for the command to complete, which should take approximately 30 seconds. Verify that **Issued** is displayed under **Status**.

#### Task 4: Verify site functionality

1. Switch to **SEA-ADM1**, in the **Internet Information Services (IIS) Manager**, right-click (or access the context menu) **Default Web Site**, and then select **Edit Bindings**.
2. In the **Site Bindings** dialog box, select **Add** and under **type**, select **https**.
3. Under **SSL certificate**, select the certificate displayed with a GUID, select **OK** and then select **Close**. The GUID will be similar to: **35B56A0F8D0AC682579BA893524EDFC6EC8FBA83**.
4. On **SEA-ADM1**, open Microsoft Edge and in the address bar, enter **http://www.contoso.com**. Verify that the website displays. Notice that **Not secure** is displayed next to **www.contoso.com**.
5. In the address bar, enter **https://www.contoso.com**. Verify that the website displays. Notice that a padlock displays next to **www.contoso.com**. This means that the website is protected using SSL.

©2019 Microsoft Corporation. All rights reserved. The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are ***not*** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.