**suProject 2: IPsec and SSH based VPNs**

[1 Configuring Windows for FTP service 1](#_Toc462397731)

[1.1 Install Internet Information Services and the FTP Service 1](#_Toc462397732)

[1.2 Configure the FTP Service 2](#_Toc462397733)

[1.3 Testing FTP service 2](#_Toc462397734)

[2 Capture non-IPsec FTP traffic with Wireshark 3](#_Toc462397735)

[3 Setting IPsec VPN for Window machines 3](#_Toc462397736)

[3.1 Setting the IPSec policy for the Windows server machine 4](#_Toc462397737)

[3.2 Setting the IPSec policy for the Windows client machine 5](#_Toc462397738)

[3.3 Test IPSec configuration 5](#_Toc462397739)

[3.4 Capture IPsec protected FTP traffic using Wireshark 5](#_Toc462397740)

[4 SSH Tunneling (port forwarding) 6](#_Toc462397741)

[4.1 Configure the VNC service 6](#_Toc462397742)

[4.2 Configure the SSH port forwarding 7](#_Toc462397743)

**Goal:** In this project, we will configure a host-to-host VPN using IPSec and SSH respectively. The purpose of this lab is to allow you to gain “hands-on” experience with using various VPNs and how they can be used to protect your network communications.

# Configuring Windows for FTP service

The article from the link is pasted here for your reference:

<http://www.wikihow.com/Set-up-an-Ftp-Server-on-Windows-Xp-Professional>

<http://support.microsoft.com/kb/323384>

https://docs.microsoft.com/en-us/iis/install/installing-publishing-technologies/installing-and-configuring-ftp-7-on-iis-7

**Summary:** This step-by-step article describes how to install and configure a File Transfer Protocol (FTP) server for anonymous access.

## Install Internet Information Services and the FTP Service (6 points)

Because FTP depends on Microsoft Internet Information Services (IIS), IIS and the FTP Service must be installed on the computer. To install IIS and the FTP Service, follow these steps.

**NOTE**: In Windows 7, the FTP Service is not installed by default when you install IIS. If you already installed IIS on the computer, you must use the Add or Remove Programs tool in Control Panel to install the FTP Service.

|  |  |
| --- | --- |
| 1. | Click **Start**, point to **Control Panel**, and then click **Programs**. |
| 2. | Click **Turn Windows features on or off**. |
| 3. | In the **Windows Features** list, expand **Internet Information Services (IIS)**, then **File Transfer Protocol (FTP)**" server. |
| 4. | Select **FTP service** and **FTP Extensibility**. |
| 5. | Click **OK**. |

IIS and the FTP service are now installed. You need to configure the FTP Service before you can use it.

## Configure the FTP Service (6 points)

To configure the FTP Service to allow only anonymous connections, follow these steps:

|  |  |
| --- | --- |
| 1. | Double click the **Internet Information Services** icon from **Administrative Tools** in **Control Panel**. |
| 2. | Expand **Server\_name**, where Server\_name is the name of the server. (see the figure below)  VirtualBox_IE8%20-%20Win7_1_28_09_2017_16_55_05.png |
| 3. | Right-click on Sites and then choose Add FTP Site. This opens the FTP wizard where you start by giving your FTP site a name and choosing the physical location for the files. Call it "Default FTP Site" with a path of "C:\inetpub\ftproot"; hit next |
| 4. | Enable Start FTP site automatically, select Allow SSL; hit next |
| 5. | Click to select the **Anonymous and Basic** check box (if it is not already selected).  Allow access to all users. |
| 6. | Click to select the **Read** boxes (if they are not already selected), and then click to clear the **Write** check(if it is not already cleared). |
| 7. | Click **Finish**. |

The FTP server is now configured to accept incoming FTP requests. Copy or move the files that you want to make available to the FTP publishing folder for access. The default folder is drive:\inetpub\ftproot, where drive is the drive on which IIS is installed (in our case, it is the C drive).

## Testing FTP service

Once FTP has been configured and started: Use nmap on your FC machine to make certain that your Windows machine has its FTP port open. If nmap command not found, use to the following to install it

yum install nmap.

Open the command line. Use your Windows client machine to make certain that you have connectivity to the FTP Server by pinging the server. (3 points)

Under the command line, use the anonymous username and any password at the FTP prompt. (3 points)

When confirmed that FTP is working properly, quit the FTP connection (bye). (2 points)

# Capture non-IPsec FTP traffic with Wireshark

On your Windows server machine:

Start capturing packets using the Wireshark.

On your Windows client machine:

Again, ping the Server machine

Again, connect to the Server machine via FTP

Enter the username and password

Once logged in – quit the FTP connection （3 points）

Stop the Wireshark capture on the Windows machine. View the Wireshark output.

Save the file as nonipsec. (3 pionts)

### Were you able to determine the source and destination port of the FTP connection? If so, what are they? (3 pionts)

### Were you able to sniff the FTP username and password? Make certain to explain this answer. (3 pionts)

# Setting IPsec VPN for Window machines

A *security policy* can be defined as a set of rules and practices that govern how an organization manages and protects its assets (which can include facilities, equipment, infrastructure or information). IT security focuses on the protection of:

* Computer systems/software
* Network connectivity
* Sensitive or confidential information

Policy-based security, then, begins by defining the organization’s philosophy and priorities in regard to protection of the above. Application of the rules and practices outlined in the policy statement is then accomplished via the technical definition of “security policy.”

In this context, a security policy is a template used to select and configure the various security mechanisms supported by the operating system or application. Modern Windows operating systems support many different types of security policies. IPsec is one of them. In this section, we will briefly introduce how to set and enable IPsec policies.

The **Local Security Policy MMC (Microsoft Management Console)** interface is used to configure security settings that apply only to the local computer. It’s accessed via the Administrative Tools menu in Control Panel. Local settings include: password policy, account lockout policy, audit policy, IPsec policy, user rights assignment, and others. Local Security Policy is not used on domain controllers; they are governed by the Domain Controller Security Policy.

## Setting the IPSec policy for the Windows server machine

On your Windows server machine: Open the MMC console and determine where to set the security policies for Local Computer (see the figure below).

******

Alter the Secure Server policy to use a preshared-key of wdYw4l2D (what do you want for lunch today) for both IP and ICMP traffic. (5 pionts)

Hint:

1. Right-click the IP Security Policies node, and then click **Create IP Security Policy**.
2. In the IP Security Policy Wizard, click **Next**.
3. Type a name and a description (optional) of the policy, and then click **Next**.
4. Click **Next**.
5. Right-click the IPsec policy, and then click **Properties**
6. Click **Add.** Create IP Security Rule Wizard. You can use the default setting.
7. Set the initial authentication method for this security rule as **Use this string to protect the key exchange**. Use wdYw4l2D as the preshared-key.

Make certain that this policy ensures that this security MUST be used.

Assign these settings on the Secure Server policy (3 pionts)

Ping the server from client machine

### What response did you get? (3 pionts)

FTP to the Server machine from the client

### What message did you receive? (3 pionts)

Quit the FTP application

## Setting the IPSec policy for the Windows client machine (4 pionts)

Now, do the same thing for your Windows client machine. Make certain that this policy ensures that this security MUST be used. Assign these settings on the Secure Server policy.

## Test IPSec configuration

On your client machine:

Ping the server from Windows client machine

### What response did you get? (3 pionts)

FTP to the Server machine from the client

### What message did you receive? (3 pionts)

Quit the FTP application

### Try to ping, ftp your Windows client and Server from your Linux machine. Can you get through? Why or why not? (3 pionts)

## Capture IPsec protected FTP traffic using Wireshark

On your Windows server machine:

Start capturing packets using the Wireshark.

On your Windows client machine:

Again, ping the Server machine

Again, connect to the Server machine via FTP

Enter the username and password

Once logged in – quit the FTP connection (3 pionts)

Stop the Wireshark capture on the Windows machine.

View the Wireshark output.

Save the file as IPsec (3 pionts)

### Were you able to determine the source and destination port of the FTP connection? Why or why not? (3 pionts)

### Were you able to sniff the FTP username and password? Make certain to explain this answer. (3 pionts)

# SSH Tunneling (port forwarding)

SSH tunneling, or Port forwarding, is a way to forward otherwise insecure TCP traffic through SSH Secure Shell. You can secure for example POP3, SMTP and HTTP connections that would otherwise be insecure. There are two kinds of port forwarding: local and remote forwarding.

Local port forwarding forwards traffic coming to a local port to a specified remote port. For example, all traffic coming to port 1234 on the client could be forwarded to port 23 on the server (host). Local port forwarding is pretty common.

Remote port forwarding does the opposite: it forwards traffic coming to a remote port to a specified local port. For example, all traffic coming to port 1234 on the server (host) could be forwarded to port 23 on the client (localhost). Remote port forwarding is uncommon.

In this lab, we will configure local port forwarding. Make sure that the firewall is turned off on both your server and client.

## Configure the VNC service

On your Fedora server side, as the root user, issue the following commands:

*yum install tigervnc-server*

*vncserver :3*

*You will require a password to access your desktops.*

*Password: (****you can type any password; you will use this password to login from the client****)*

*Verify:* (2 pionts)

Then, verify the vnc service is running: (3 pionts)

*netstat -tulnp | grep X*

*tcp 0 0 0.0.0.0:****5903*** *0.0.0.0:\* LISTEN 4361/Xvnc*

*tcp 0 0 0.0.0.0:6000 0.0.0.0:\* LISTEN 1755/Xorg*

*tcp 0 0 0.0.0.0:6003 0.0.0.0:\* LISTEN 4361/Xvnc*

*tcp 0 0 :::6000 :::\* LISTEN 1755/Xorg*

*tcp 0 0 :::6003 :::\* LISTEN 4361/Xvnc*

Note that, please record the port number that Xvnc uses, here it uses 5903. Yours may vary.

Hint: If you use Fedora 18. You may need to add*-session optional pam\_systemd.so* to /etc/pam.d/runuser-l and modify vncserver@:<display>.service file. Change the Type from forking to simple, add an -fg parameter to the vncserver command in ExecStart and delete the ExecStop line.

On your Linux client side, as the root user:

*yum install tigervnc*

Open the Wireshark program and start a new capture.

*wireshark &*

Now, connect to the VNC server

*vncviewer server\_ip :3*

Login with the password you have just created. (3 pionts)

After you log in, close the VNC terminal and stop the Wireshark capture. Verify that you can see the authentication procedure and information exchange in the captured data. (3 pionts)

## Configure the SSH port forwarding

Hint: Open ssh service and disable firewalld on your server and cient.

On your client side, as the root user, issue the following commands: (3 pionts)

*ssh -L 5911:127.0.0.1:5903 -N server\_ip*

You will be prompted for the root password of the server. Please note that you may need to modify 5903 accordingly (the port number observed in section 4.1).

Open another terminal; verify that your loopback address is listening on port 5911. (3 pionts)

*netstat -tnlp| grep ssh*

*tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 1330/sshd*

***tcp 0 0 127.0.0.1:5911 0.0.0.0:\* LISTEN 3347/ssh***

*tcp 0 0 :::22 :::\* LISTEN 1330/sshd*

Open the Wireshark program and start a new capture.

Now you can VNC connect to the local port 5911: (3 pionts)

*vncviewer localhost:5911*

Login with the password created previously. If are able to login correctly, the port forwarding is working.

Go to your server side, verify that the ssh connection is established: (3 pionts)

netstat -tnp | grep ssh

*tcp 0 0 127.0.0.1:59442 127.0.0.1:5901 ESTABLISHED 7623/sshd: root*

*tcp 0 0 10.0.100.103:22 10.0.100.104:55490 ESTABLISHED 7623/sshd: root*

Close the VNC terminal and stop the Wireshark capture. Verify that you cannot see the authentication procedure and information exchange. (2 pionts)

### Explain how SSH tunneling (port forwarding) works (3 pionts)

To stop your vncserver on the service side, type: (2 pionts)

*vncserver -kill :3*