Toolbox: Encrypt FTP via IPsec in 10 Steps

As ubiquitous as FTP is, many security and IT administrators shun it because FTP traffic passing between the client and server is unencrypted and visible to any network snooper who might be listening. Before you resort to cobbling together a Win32 port of OpenSSH (a freeware version of the Secure Shell—SSH—suite of network-connectivity tools) or spending thousands of dollars for a commercial version of SSH, consider using IPsec to encrypt your FTP traffic. Together, FTP and IPsec provide a secure and relatively easy-to-deploy solution for remote-console access for Windows Server 2003-12 servers. Although configuring IPsec can be complicated, here I provide 10 quick, straightforward steps to follow for encrypting FTP over IPsec. You can also extend these examples for encrypting other network traffic to suit your own security needs.

A Few Preliminaries.
The sample configuration that I'll walk you through uses Kerberos—the Windows IPsec default authentication method—which means that your client and server must reside in the same or trusted domains. IPsec supports alternative authentication mechanisms (e.g., certificates) that you can use if Kerberos isn't an option for your domain. However, such mechanisms can be trickier to set up and require an existing public key infrastructure (PKI).

When you configure IPsec for the first time, the IPsec wizards might seem daunting. One wizard invokes another wizard, which invokes yet another. But after you've created the objects once, the interaction of the elements will make sense. To encrypt FTP traffic over IPsec, you'll create these objects:

- IPsec policy (steps 3 and 4)
- IPsec security rule (steps 5 and 6)
- IP filter list (step 7)
- filter action (step 9)

Windows 2003-12 includes helpful tools for troubleshooting failed IPsec connections. One such tool is the Microsoft Management Console (MMC) IP Security Monitor snap-in, which shows you the filters, policies, and security associations for both Main Mode and Quick Mode IPsec. Also, you can use a network sniffer to watch network traffic as the IPsec connection between the client and server is negotiated. Although the sniffer doesn't display the contents of the encrypted traffic, you can see the client and server setting up the IPsec connection via Internet Security Association and Key Management Protocol (ISAKMP, TCP port 500).

To create the IPsec Policy
To encrypt FTP traffic for your domain, follow these steps:

1. On each server that you want to manage by using FTP, install FTP and open the Services applet in Administrative Tools and enable the FTP service to start up automatically, then start the service.

2. Create a new Group Policy Object (GPO) and link it to the organizational unit (OU) containing the computers (clients and servers) on which you want to require encrypted FTP sessions. If you choose, you can link this GPO at the domain level for every computer in the domain to encrypt the FTP sessions.

3. Edit this new GPO by using Group Policy Editor (GPE). Navigate to Computer Configuration, Windows Settings, Security Settings. Right-click *IP Security Policies on Active Directory (domain)* and click *Create IP Security Policy* to launch the IP Security Policy Wizard.

4. Walk through the wizard by following these steps:

- Name the policy (e.g., *IPsec FTP Policy*)
- Leave the default *Activate the default response rule* check box as is.
- Leave the Default Response Rule Authentication Method set as *Active Directory default (Kerberos V5 protocol).*
- When you're at the end of the wizard, select the *Edit properties* check box to configure the policy. Click Finish to exit the wizard.

Create the Security Rule and IP Filter List

5. Next you'll add a new IP Security rule that encrypts FTP traffic. Create the rule by clicking the Rules tab of your newly created policy's properties dialog box. Click Add to start the Security Rule Wizard.

6. Proceed through the Security Rule Wizard as follows:

- Leave the default *This rule does not specify a tunnel* radio button selected.
- Leave the default *All Network Connections* radio button selected.
- When you're prompted for the IP filter list, click Add to create a new IP filter list.

7. The IP filter list defines the protocol and addresses that the IPsec rule uses. In the New IP Filter List dialog box that's displayed, name the new IP filter list (e.g., FTP) and click Add to run the IP Filter Wizard. Proceed through the wizard by entering or selecting the following information:

- Enter a description—for example, *FTP (TCP port 21)*—and make sure that the *Mirrored* check box is selected. Match packets with the exact opposite source and destination addresses.
- In the *Source address* drop-down box, select the source address as *Any IP address.*
- In the *Destination address* drop-down box, select the destination address as *Any IP address.*
- Specify the protocol type as TCP.
- Click the *From any port* radio button.
- Click the *To this port:* radio button and enter 21 in the text box (to specify the FTP port, TCP port 21).

8. Click OK to close the new IP Filter List dialog box, which returns you to the Security Rule Wizard in step 6. Click the radio button next to your newly created IP filter list (e.g., FTP) and click Next.

Create the Filter Action

9. Now we need to create the filter action. To do so, click Add, which launches the Filter Action Wizard. Proceed through the wizard as follows:

- Enter a name (e.g., *Encrypt data*).
- Click the *Negotiate security* radio button.
- Click the *Do not communicate with computers that do not support IPsec* radio button.
- Click the *Integrity and encryption* radio button.
- Select the *Edit properties* check box and click Finish to display the Filter Action properties.
- Select the *Accept unsecured communication, but always respond using IPsec* check box and click OK to exit the Filter Action properties dialog box.

Accepting unsecured communications is necessary because when a client computer initiates a FTP session, it first tries to do so by using TCP port 21. The IPsec-protected server needs to recognize and accept this unsecured request but then immediately respond by setting up IPsec communications. Without this security negotiation, the client can't connect to the server. The benefit of this filter-action configuration is that it lets your clients still connect to routers, switches, and other non-IPsecenabled FTP servers if they need to.

10. Exiting the Filter Action properties dialog box and wizard returns you to the Security Rule Wizard. Click the radio button next to your newly created filter action (e.g., Encrypt Data) and click Next. Leave the authentication method for your new rule at the default of *Active Directory (i.e., Kerberos V5 protocol),* then exit the wizard.

You've now configured the core components of an IPsec policy. You can review the details of this policy by viewing the policy's properties pages, which Figure 1 shows, or click OK twice to exit the policy's properties.

Assign the IPsec Policy ... and You're Done!
You're now ready to assign the policy. Return to GPE and select *IP Security Policies on Active Directory (domain).* In the right pane, right-click your new IPsec FTP policy and select Assign. Force the GPO update by running the Gpupdate command on each computer running the FTP server (or you can wait for the GPO to replicate). You must run Gpupdate on both the client and server.

IPsec used in conjunction with FTP dramatically improves FTP security. Running FTP over IPsec might not be ideal for every organization because of the additional requirement and complexity of setting up an Active Directory (AD) GPO. But if you manage a number of Windows servers and avoided FTP in the past because of its nonsecurity, IPsec lets you consider it as another method to support remote administration of your servers.