

Creating an L2TP/IPSEC VPN Server using Windows 2003 and ISA Server

Software Required

- Microsoft Windows 2003 Enterprise Edition
- Microsoft ISA Server 2004 or 2006
- Windows XP, Windows Vista or Windows 2000 Pro.

Hardware Required

- Ideally at least two servers. One server should have two NICs, one for the internal network, one for the internet connection.
- Two workstations for testing purposes

Services Required

- Certificate Services
- IIS
- Active Directory
- IAS (RADIUS)
- RRAS (Configured by ISA)
- Active Directory/Group Policy

Procedure

Install Windows Server 2003 Enterprise Edition on your first server. Promote it to a DC if you desire, at the very least join it to your domain. Install Certificate Services, IIS and IAS on the server. We shall call this server AUTHSRV. Make sure that your Domain Level is set to Windows 2003 Native to make administration of remote access policies simpler.

Install Windows Server 2003 Enterprise or Standard Edition on your second server. Join it to the domain. Install ISA Server 2004 or 2006 on the server. This server shall be called VPNSRV. Make sure you set up firewall rules that localhost can talk to localnetwork and vice versa.

Install Windows 2000/XP/Vista on both workstations.

On AUTHSRV, open the IAS console. Right click on Internet Authentication Service (Local) and press Register in Active Directory. Go to RADIUS clients. Right click, press New RADIUS client. Type in a name in the Friendly name box (e.g. "VPN Server") and the IP address of your VPN server in the client address box. Keep the RADIUS vendor as RADIUS Standard and type in a password in the shared secret box. Make it as strong and as long as possible, make a note of it. Press the Finish button.

Open ADUC. Create a user group called "VPN Users" or something similar. Add your user or some test users to this group. Go back to the IAS console and go to Remote Access Policies. Create a new policy, follow the wizard to set up a common access scenario and give the policy a name. Choose VPN, press next. Put the group you just created into the group box, press next. Choose the MS CHAP

v2 authentication protocol, press next. Disable all but the strongest encryption, press next then press finish. If you want to increase security further, you could use EAP and use smartcards to authenticate but that is well beyond the scope of this article.

The following is necessary to allow non domain PCs to connect to your VPN. Open the Certification Authority console. Expand the tree. Right click on Certificate Templates and click Manage. The Certificate Template MMC will open. Find IPSEC (Offline Request), right click on it and press Duplicate Template. Type "VPN Access Certificate" or something similar in the Template Display Name and check the "Publish in AD" box. Go to the Request Handling box and press the CSPs button. Choose the "Requests can use any CSP" option and press OK. If you want to be able to manually approve certificate requests, go to the Issuance Requirements tab and check the CA Certificate Manager Approval box. Finally, go to the Security tab, add the group that your users are in (Students, teachers, domain users, whatever) and allow read, enrol and autoenrol. Go back to the CA MMC. Right click on Certificate Templates, go to New and choose New Certificate Template to Issue. Find the template you just created, click on it and press OK.

The following is necessary if you want your domain PCs to automatically obtain certificates to connect to the VPN. Useful for teacher laptops. Open the GPMC. Either edit the default domain policy (Not recommended) or create a new GPO attached to the OU your workstations are located in. Go to Computer Configuration/Security Settings/Public Key Policies/Automatic Certificate Request Settings. Right click on Automatic Certificate Request Settings and press New/Automatic Certificate Request. Follow the wizard, for the certificate type, choose Computer. Run the wizard again, choose IPSEC. Run "GPUPDATE /force" on the DC.

The following instructions have been tested on ISA 2006. I believe that ISA 2004 is broadly similar but I do not have a copy to hand to test it with so I cannot be certain. On VPNSRV, open the ISA server console. Go to the VPN section and follow the steps. It's your choice if you want to use a static IP Address pool or DHCP but I'd recommend DHCP for simplicity's sake. Click on the Enable VPN access link and check the box. Put in the maximum amount of clients you want to use and press OK.

Click on the RADIUS Server link. Check both boxes and press the RADIUS server button. Fill out the form, put in the server IP address, shared secret etc.

Click on the Verify Firewall Properties link. Disable PPTP and enable L2TP/IPSEC. Apply the configuration.

Open Internet Explorer. Browse to <http://AUTHSRV/certsrv>. Click on request a certificate, click Advanced Certificate Request, create and submit. Choose the template you created earlier, put the FQDN of the server into the Name field. Make sure that the key is marked as exportable and check the "Store in local computer cert store" box. Say "Yes" to any error dialogues that appear and install the certificate when prompted. Restart the ISA server. This should be all that is necessary to get a L2TP/IPSEC based VPN going.

Testing

For testing purposes, you need two XP workstations. Make sure that one is not joined to the domain and does not have any domain issued certificates and that it does not trust your internal CA.

Connect it to the “internet” segment of your network for testing. It is probably best if you use a clean XP image which has never been connected to the network to make sure that there is nothing on it which will pollute your testing results.

The other XP workstation at first needs to be joined to your main network segment and needs to be joined to the domain. Make sure it downloads the certificates and then join it to your “Internet” network segment. Create a VPN connection and open it. Press the Properties button, go to the Networking tab and change the VPN type to L2TP/IPSEC. Enter a username and password that is a member of the group you created previously and press connect. All being well, you should connect to the VPN, be assigned an IP address and be able to browse network resources.

You now need to test whether it works for non-domain members. To do this, you need to request an IPSEC certificate and export it to the non domain member. You also need to export a CA trust certificate to the non domain member to make it work.

Put the domain connected XP workstation back onto the main network segment or connect to the main network using the VPN connection. Browse to <http://authsrv/certsrv>. Go to the Certificate request page and request an advanced certificate. Choose the certificate template you requested earlier, type a name into the box, make sure the key is exportable, place the cert in the machine store, submit the request and install the cert when prompted. Go to the Certificate Services homepage, click Download a CA certificate, certificate chain, or CRL then Download CA certificate. Save the CA certificate to a removable device. The CA certificate will be a CER file. Open MMC, add the Certificates snap-in and expand the tree and go to the Personal/Certificates folder. Right click on the cert you just created, go to All tasks and press Export. Make sure you export the private key and type in a password for it when prompted. Save the certificate to a removable device. The exported certificate will be a PFX file.

Put the removable device into the non-domain workstation. Import the PFX file into the Personal certificate store and the CER file into the Trusted Certification Authority store. Create a VPN connection again making sure that the L2TP connection VPN type is selected. Press connect and all being well you should connect.