

Configuring Windows XP/Vista L2TP client & Zeroshell

Basics:

Boot from zeroshell CD then log into your zeroshell box. With the default image/configs it is ready to accept L2TP connections by simply enabling the check box in the /NETWORK/VPN/Host-to-LAN (L2TP/IPSEC) GUI menu and USERS/RADIUS enable. Watch for the radius warning.

Zeroshell Net Services interface showing the L2TP/IPSec configuration page. The 'Enabled' checkbox is circled in red. The page title is "L2TP over IPsec with X.509 IKE and MSCHAPv2 client authentication". The status is "DOWN". There are buttons for "Show Clients", "IPSec Log", and "Radius Log". Below is the "IPsec IKE Configuration" section with "X.509 Host Certificate" set to "Local CA" and "OU=Hosts, CN=portal1.premier.hh". There is a "Check CRL" checkbox and buttons for "Imported" and "Trusted CAs". The "Client IP Address Assignment" section shows a range from 172.16.24.40 to 172.16.24.45. The "Routing Method" section has radio buttons for "Normal", "ProxyARP", and "Source NAT" (selected), and a "NAT-T" checkbox. A "Some Notes" section at the bottom explains the VPN configuration.

Zeroshell is ready now it's time to setup the clients. The "admin" account on zeroshell is created by default we'll just use that one for demonstration purpose.

Now you want to create a host file certificate for each computer that will be accessing your L2TP vpn server (i.e. zeroshell box). Click on NETWORK/Hosts/Add

Zeroshell Net Services interface showing the "New Host" form. The "Add" button in the top navigation bar is circled in red. The "Submit" button at the bottom right of the form is also circled in red. The form fields include Hostname, Domain, Description, and Administrator's E-Mail. The "Kerberos 5 Authentication" section has radio buttons for "Enabled" (selected) and "Disabled". A red arrow points to the "Submit" button with the text "Just fill in the blanks with whatever you want and then click 'Submit'".

Now select your user "admin" account USERS/Users/View and make sure L2TP is checked so that this user is allowed to connect.


ZEROSHELL Net Services Release 1.0.beta11b

CPU (2) Intel(R) Core(TM)2 Duo CPU E6550 @ 2.33GHz 2327MHz Refresh
 Uptime 0 days, 5:36
 Load Avg 0.01 0.01 0.00 Graphics

Logout Reboot Shutdown

USERS List **View** Add Edit Delete X509 Kerberos 5

Entries found: 1 Search Primary Group

Username	Group	Description	E-mail
 admin	nobody	System Administrator	?

SYSTEM
 • Setup
 • Logs
 • Utilities

USERS
 • Users
 • Groups
 • LDAP / NIS
 • RADIUS
 • Captive Portal

NETWORK
 • Hosts
 • Router
 • DNS
 • DHCP
 • VPN
 • QoS
 • Wireless
 • Net Balancer

SECURITY
 • Kerberos 5
 • Firewall
 • X.509 CA
 • HTTP Proxy

ToDo List
 • IMAP Server
 • SMTP Server

ZEROSHELL Net Services Release 1.0.beta11b

CPU (2) Intel(R) Core(TM)2 Duo CPU E6550 @ 2.33GHz 2327MHz Refresh
 Uptime 0 days, 5:36
 Load Avg 0.01 0.01 0.00 Graphics

Logout Reboot Shutdown

USERS List View **Add** Edit Delete X509 Kerberos 5

System Administrator (admin)

Account
 Username uid Primary Group gid

Home Directory Default Shell bash sh tcsh other

User Information
 Firstname Lastname Organization

Description E-Mail Phone

User Password
 Password
 Confirm

Enabled Services
 Kerberos 5 Authentication
 Host-to-Lan VPN (L2TP/IPsec)
 802.1X Access (VLAN)

SYSTEM
 • Setup
 • Logs
 • Utilities

USERS
 • Users
 • Groups
 • LDAP / NIS
 • RADIUS
 • Captive Portal

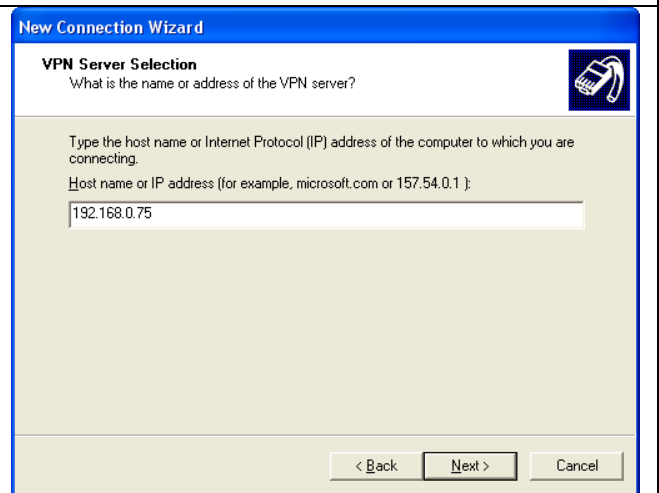
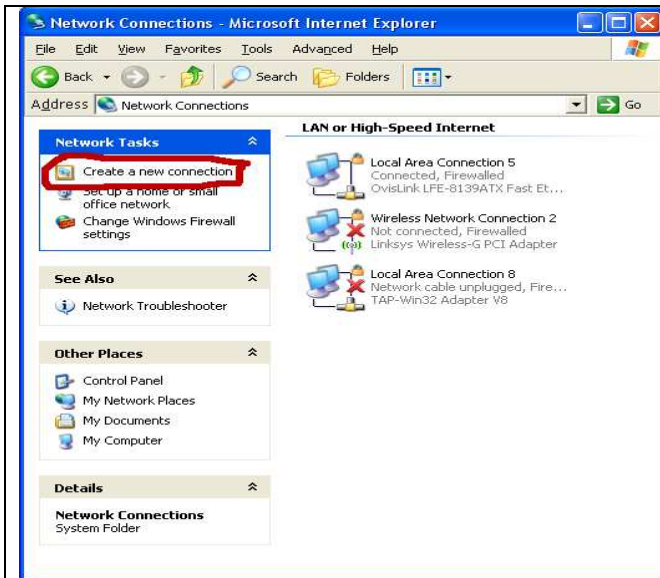
NETWORK
 • Hosts
 • Router
 • DNS
 • DHCP
 • VPN
 • QoS
 • Wireless
 • Net Balancer

SECURITY
 • Kerberos 5
 • Firewall
 • X.509 CA
 • HTTP Proxy

ToDo List
 • IMAP Server
 • SMTP Server

That's all with zeroshell. Now move on to your clients PC. In your windows XP computer "Create a new connection" from Control Panel/Network Connections. In windows Vista "Set up a connection or network" from Control Panel/Network and Internet/Connect to a network.

Screenshots of windows XP below



That's the end of the basics.

Screenshots of Vista are essentially the same so I'm not going to put them here.

Preparation – Download all your certificates from the machine you will be connecting the L2TP session or place them on a thumbdrive. You will need the host certificate that you created earlier on zeroshell for your computer and also the zeroshell CA or root Certificate of Authority.

Go to your zeroshell log in screen to get the certificates you need. You can click on “CA” to download the root certificate and then “Hosts” to get your certificate for your computer. You don’t need to be logged on to the zeroshell box, in fact it’s better that you’re not logged on.



For the root CA it is important (on windows machines) to export the certificate with the *.DER file extension and **NOT THE *.PEM** file. Now under “Hosts” choose your host certificate and export the PKCS#12 (PFX) file.

Advanced:

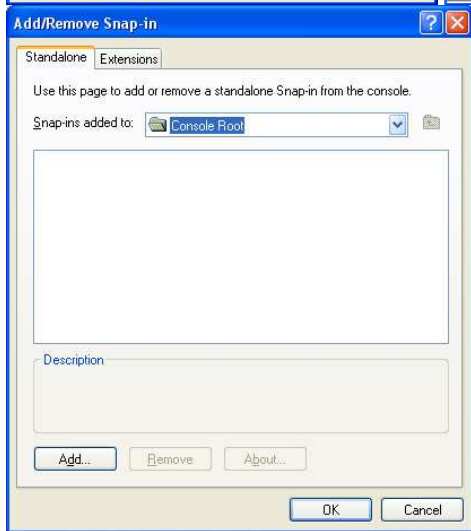
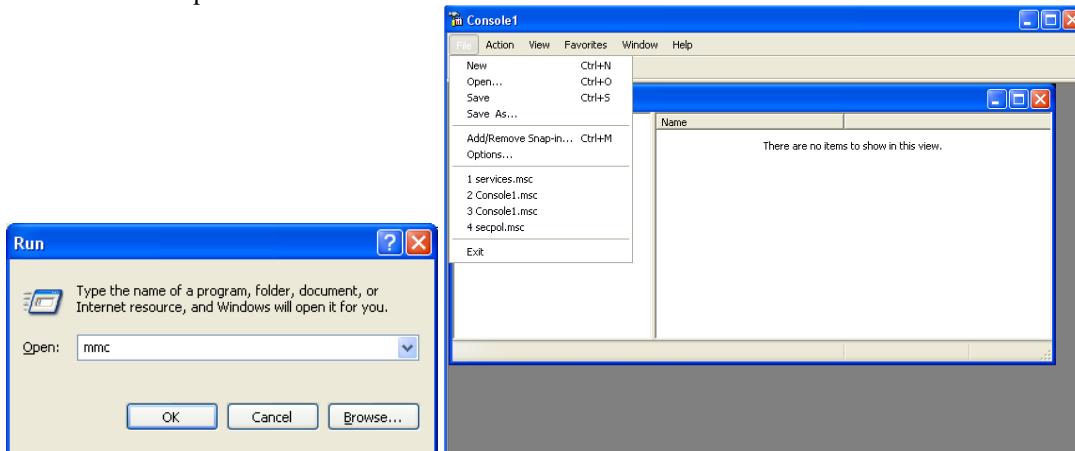
To complete the following you should be logged on an Administrator account on your client PC.

I will assume you did everything correct with the zeroshell CA and exported your host certificate (pkcs #12, der or pem file to your remote computer, example *hostname.pfx*) and now you want to configure windows XP or Vista computer.

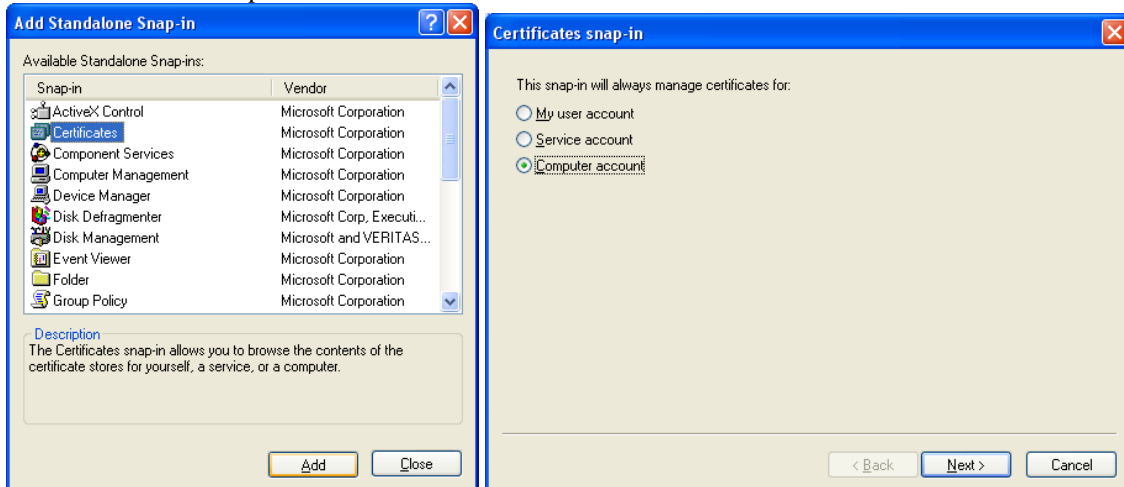
Note: For the certificate store windows will either default to use option "Automatically select the certificate store based on the type of certificate" or "Place all certificates in the following store". We're talking about windows here so if that options doesn't import the certificate well use the other option. The object is to get the certificate imported into the correct store.

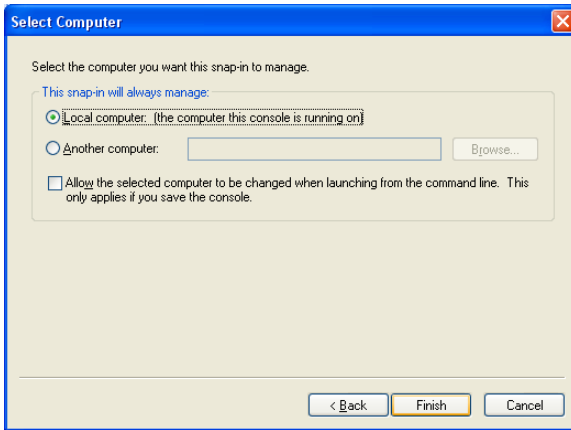
Part 1 of 4

Log on an Administrator Account and use the Run. Type "MMC" and when the console opens click, File-Add/Remove Snap-in.

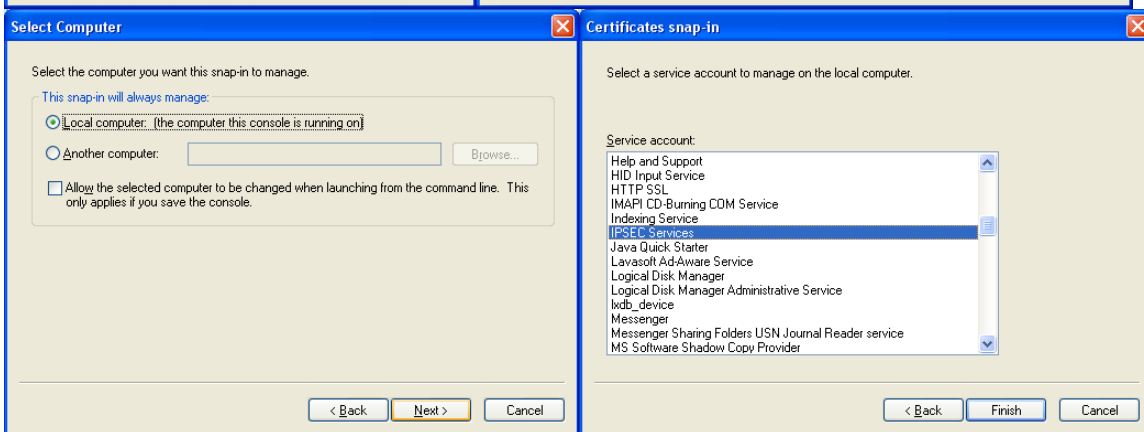
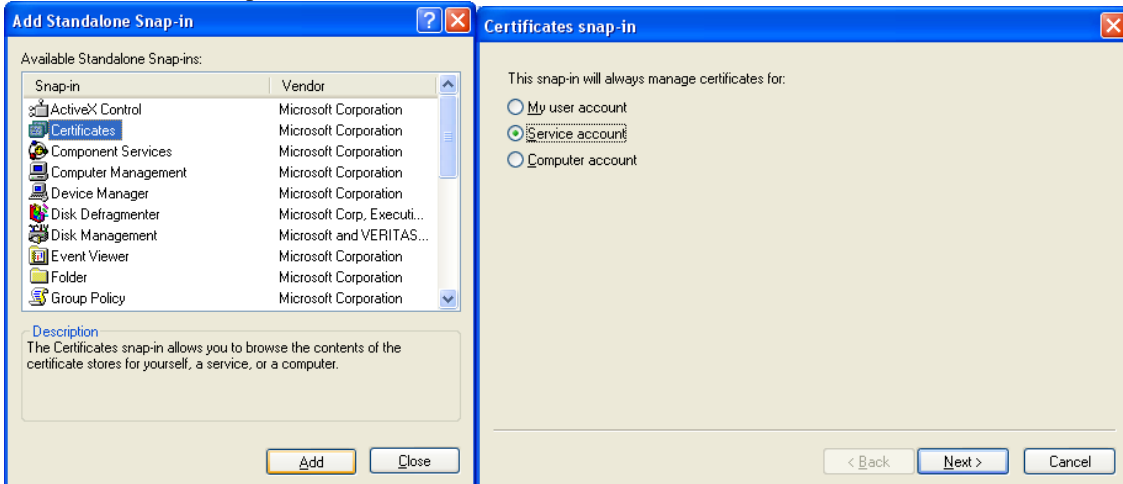


Click Add-Certificates-Add-"Computer Account"
Click Next-Local Computer-Finish

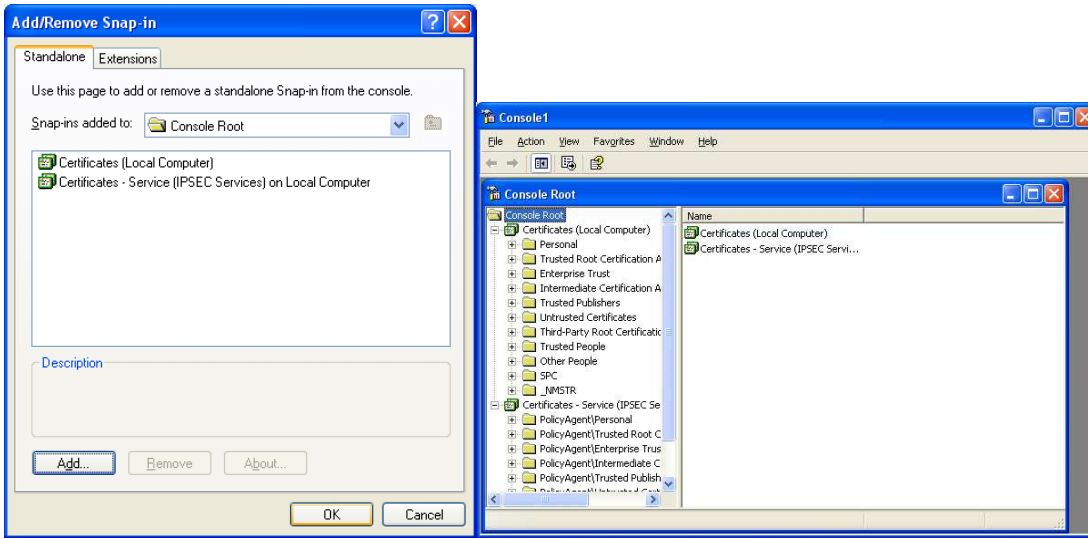




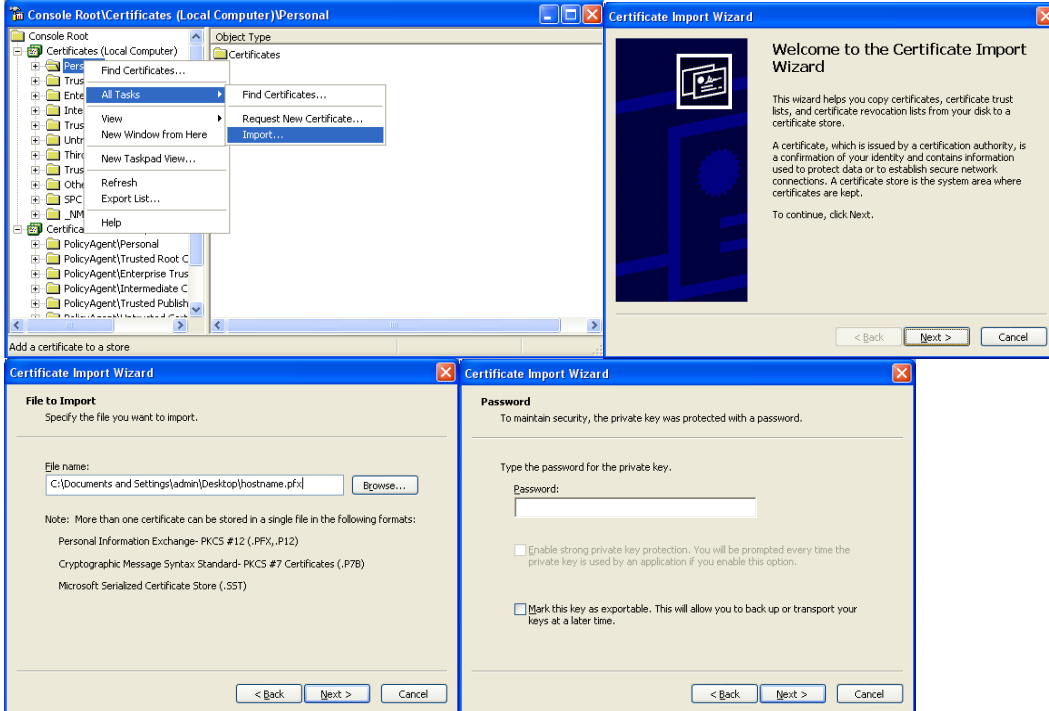
Once again,
 Click Add-Certificates-Add-"Service Account"
 Click Next-Local Computer-Next-IPSEC Services-Finish

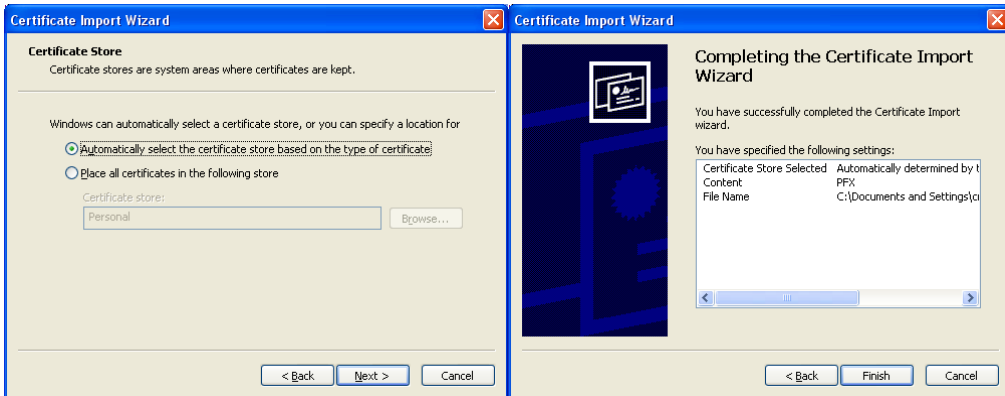


Now
 Click OK, Expand "Certificates(Local Computer)"

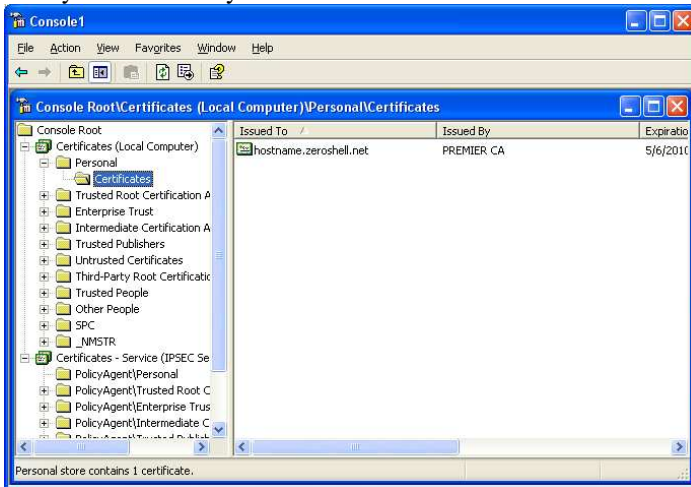


Right Click Personal-All Tasks-Import...-"hostname.pfx"-Next-Next-Automatically Select Certificate Store-Next-Finish





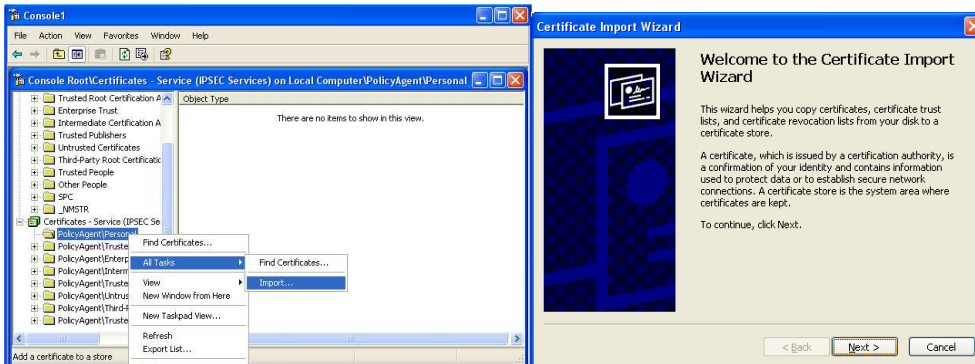
Expand "Certificates(Local Computer)"-Personal-Certificates
 Now you should see your "hostname"

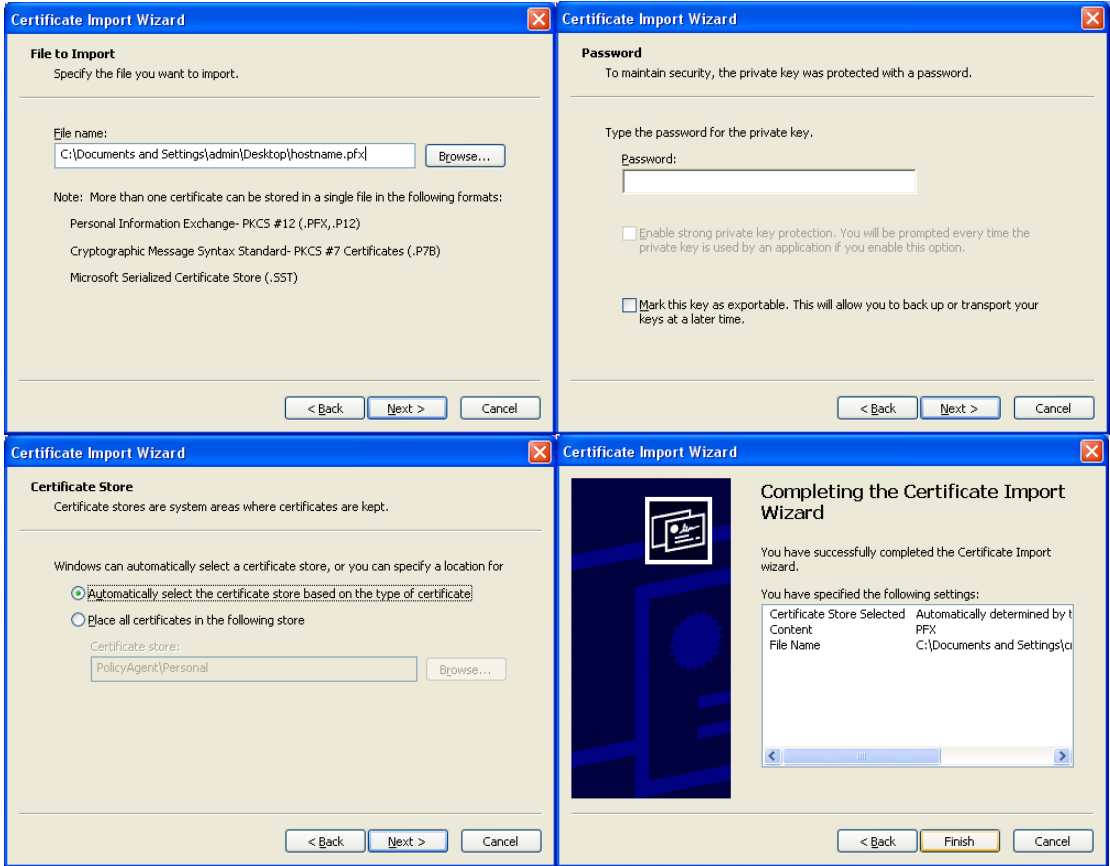


Part 2 of 4

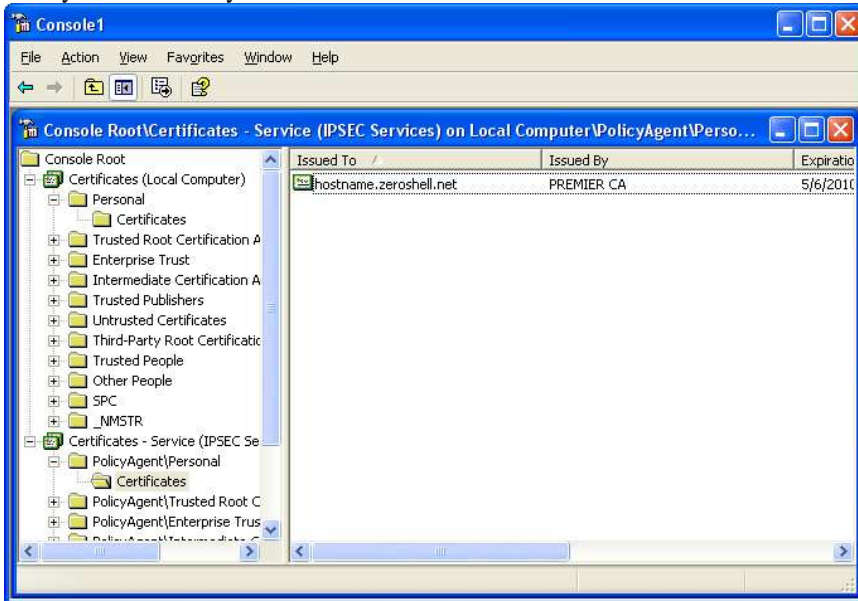
Now

Click OK, Expand "Certificates - Service (IPSEC Services) on Local Computer"
 Right Click PolicyAgent\Personal-All Tasks-Import...-"hostname.pfx"-Next-Next-Automatically Select
 Certificate Store-Next-Finish





Expand "Certificates - Service (IPSEC Services) on Local Computer"-PolicyAgent\Personal-Certificates
 Now you should see your "hostname"



Part 3 of 4

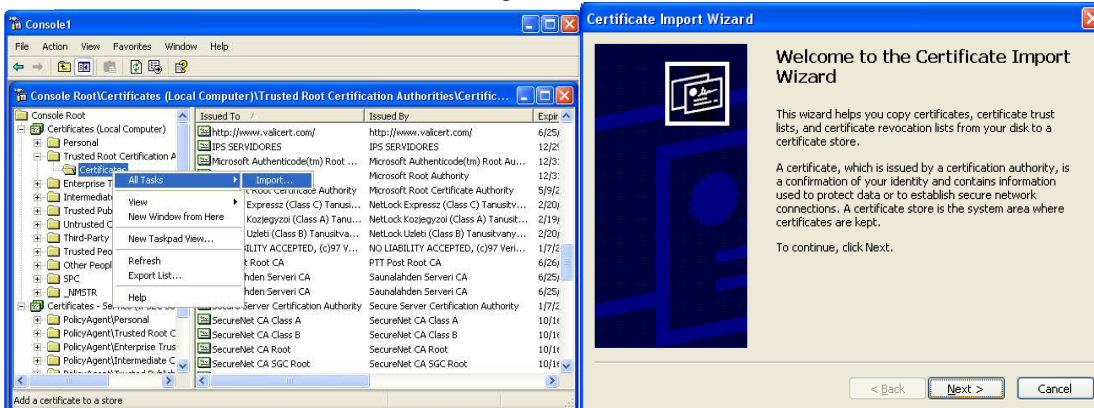
Last detail you need to import is the Trusted Root Certification Authorities or your "Zeroshell CA".

Easy method is to:

Export the der or pem file from your Zeroshell CA to your computer (Zeroshell_CA.der)

Expand "Certificates(Local Computer)"

Right Click Trusted Root Certification Authorities-Certificates-All Tasks-Import...-"Zeroshell_CA.der"-
 Next-Next-Place all certificates in the following store-Trusted Root Certification Authorities-Next-Finish



Certificate Import Wizard

File to Import
Specify the file you want to import.

File name:
C:\Documents and Settings\admin\Desktop\Zeroshell_CA.der [Browse...]

Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX, .P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)

< Back Next > Cancel

Password
To maintain security, the private key was protected with a password.

Type the password for the private key.
Password: []

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

< Back Next > Cancel

Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

Automatically select the certificate store based on the type of certificate

Place all certificates in the following store

Certificate store:
Trusted Root Certification Authorities [Browse...]

< Back Next > Cancel

Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the
Content	Certificate
File Name	C:\Documents and Settings\o

< Back Finish Cancel

Security Warning

 You are about to install a certificate from a certification authority (CA) claiming to represent:
ZeroShell Example CA

Windows cannot validate that the certificate is actually from "ZeroShell Example CA". You should confirm its origin by contacting "ZeroShell Example CA". The following number will assist you in this process:
Thumbprint (sha1): 99B671C1 291EAD02 0EB8547C 5BEC02D2 564F9A36

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

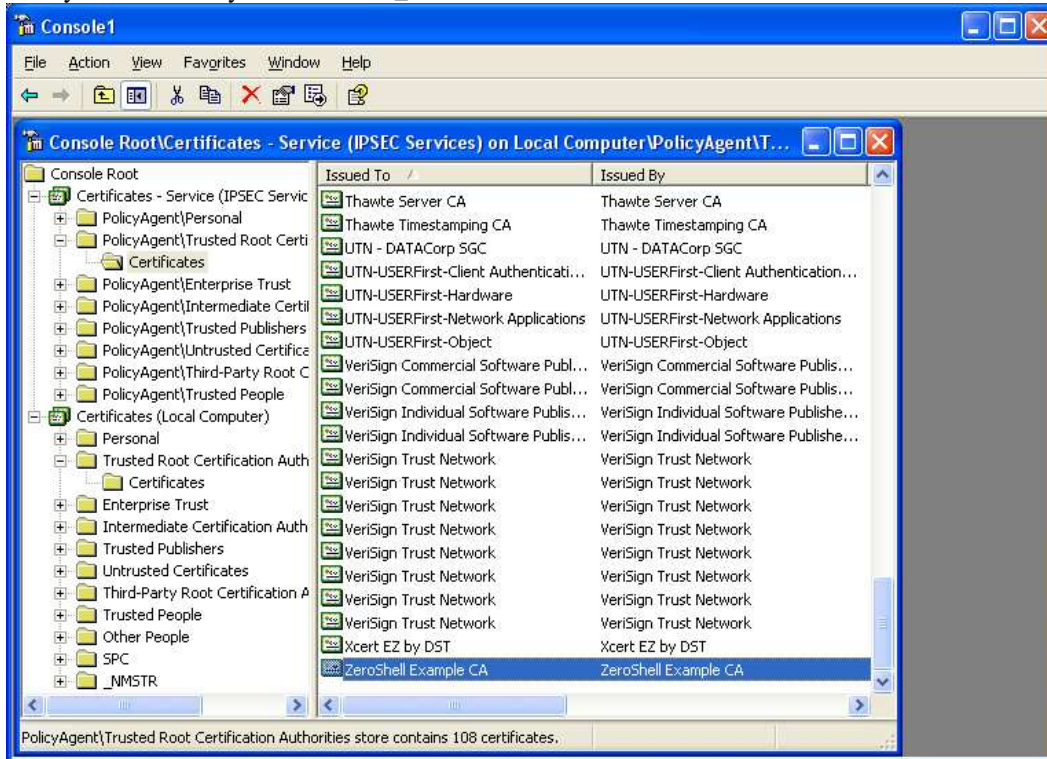
Do you want to install this certificate?

Yes No

Now

Expand "Certificates(Local Computer)"-Trusted Root Certification Authorities-Certificates

Now you should see your "Zeroshell_CA"



_____ Part 4 of 4 _____

Review:

You should see the hostname of your computer in 2 places,

[Certificates\(Local Computer\)-Personal-Certificates](#)

&

[Certificates - Service \(IPSEC Services\) on Local Computer-PolicyAgent\Personal-Certificates](#)

You should see the Zeroshell_CA in 2 places

[Certificates \(Local Computer\)-Trusted Root Certification Authorities-Certificates](#)

&

[Certificates - Service \(IPSEC Services\) on Local Computer-PolicyAgent\Trusted Root Certification Authorities-Certificates](#)

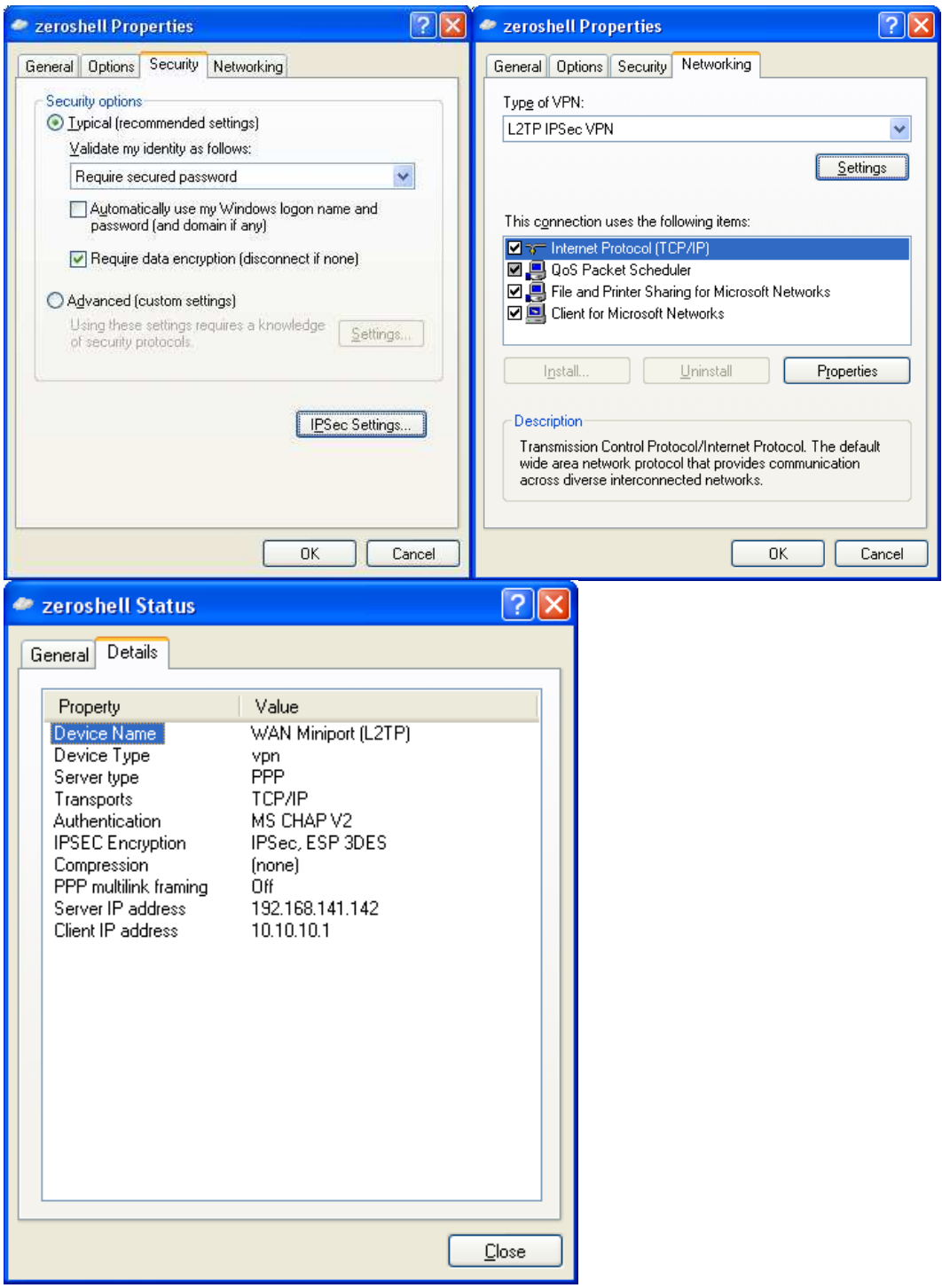
Note: When you add the Zeroshell_CA to the Certificates(Local Computer) it gets added by default to Certificates - Service (IPSEC Services) but if it doesn't you need to manually add it like we did with the other ones. *When I say manually I mean instead of letting the certificate store automatically get selected instead import it directly to the correct certificate store and use "Place all certificates in the following store" option or the default windows selects.*

Note: After completing these steps you can Create a vpn connectoid for Windows Vista & Windows XP with the default settings. In the Networking tab you should select L2TP IPSec VPN. Under Security use Typical(recommended settings) with checkbox Require data encryption (disconnect if none).

Note: Hosts should have same domain as the zeroshell box unless you know what you're doing with Kerberos 5 domain/realm trust relationships.

Click the vpn shortcut we created earlier.





The End