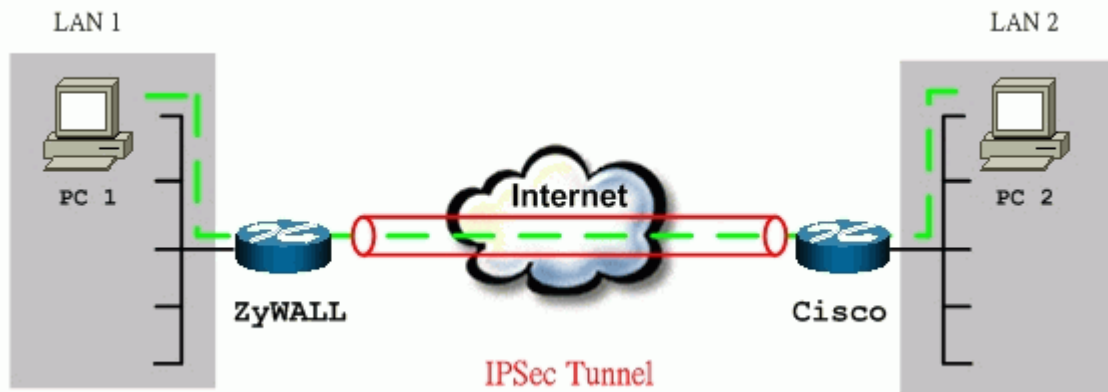


ZyWALL to Cisco Tunneling

This page guides us to setup a VPN connection between ZyWALL and Cisco router. As the figure shown below, the tunnel between ZyWALL and Cisco Router ensures the packets flow between them are secure. To setup this VPN tunnel, the required settings for ZyWALL and Cisco Router are explained in the following sections.



The IP addresses we use in this example are as shown below.

LAN 1	ZyWALL	CISCO	LAN 2
192.168.1.0/24	LAN: 192.168.1.1 WAN: 172.21.10.50	LAN: 192.168.2.1 WAN: 140.113.10.50	192.168.2.0/24

Note:

1. When using Cisco Router to establish VPN, back-to-back connection is not applicable. In other words, the WAN IP of ZyWALL and Cisco router can't be in the same subnet.

2. If the WAN IP of ZyWALL is also dynamic IP, we enter **0.0.0.0** as its **My IP Address**. When this IP is given by ISP, it will update to this field.

1. Setup ZyWALL

1. Login ZyWALL by giving the LAN IP address of ZyWALL in URL field. Default LAN IP is **192.168.1.1**, default password to login web configurator is **1234**.
2. Go to SECURITY->VPN->Press Add button
3. check **Active** check box and give a name to this policy.

4. Select **IPSec Keying Mode** to **IKE** and **Negotiation Mode** to **Main**, as we configured in Cisco.
5. In Local section, select the Address Type to **Sunbnet Address**. Specify the **network IP** of ZyWALL's LAN segment in IP Address Start field and the **subnet mask** in End/Subnet Mask field.
6. In Remote section, select the Address Type to **Sunbnet Address**. Specify the **network IP** of peer's LAN segment in IP Address Start field and the **subnet mask** in End/Subnet Mask field.
7. Choose Local ID type as **IP**, and **My IP Addr** is the **WAN IP of ZyWALL**.
8. Choose Remote ID type as **IP**, and **Secure Gateway IP Addr** is the remote secure gateway IP, that is **Peer's WAN IP** in this example.
9. Select **Encapsulation Mode** to **Tunnel**.
10. Check the **ESP** check box. (AH can not be used in SUA/NAT case)
11. Select **Encryption Algorithm** to **DES** and **Authentication Algorithm** to **MD5**, as we configured in Cisco.
12. Enter the key string **12345678** in the **Preshared Key** text box, and click **Apply**.

See the screen shot:
VPN - EDIT VPN RULE

Property	
<input checked="" type="checkbox"/> Active	
<input type="checkbox"/> Keep Alive	
<input type="checkbox"/> NAT Traversal	
Name	VPN
Key Management	IKE
Negotiation Mode	Main
Encapsulation Mode	Tunnel
DNS Server (for IPSec VPN)	0.0.0.0

Extended Authentication	
<input type="checkbox"/> Enable Extended Authentication	
<input checked="" type="radio"/> Server Mode	(Search Local User first then RADIUS)
<input type="radio"/> Client Mode	
User Name	
Password	

Local Policy	
Address Type	Subnet Address
Starting IP Address	<ZyWALL LAN>
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0

Remote Policy	
Address Type	Subnet Address
Starting IP Address	<Peer LAN>
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0

Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key	12345678
<input type="radio"/> Certificate	auto_generated_self_signed_cert (See My Certificates)
Local ID Type	IP
Content	
Peer ID Type	IP
Content	

Gateway Information	
My IP Address	<ZyWALL WAN>
Secure Gateway Address	<Peer WAN>

IPSec Algorithm	
<input checked="" type="radio"/> ESP	<input type="radio"/> AH
Encryption Algorithm	DES
Authentication Algorithm	MD5
	Authentication Algorithm MD5

You can further adjust IKE Phase 1/Phase 2 parameters by pressing **Advanced** button.

The screenshot displays a configuration window for IKE Phase 1 and Phase 2. The interface is divided into two sections: Phase 1 and Phase 2. Phase 1 settings include Negotiation Mode (Main), Encryption Algorithm (DES), Authentication Algorithm (MD5), SA Life Time (Seconds) (28800), and Key Group (DH1). Phase 2 settings include Active Protocol (ESP), Encryption Algorithm (DES), Authentication Algorithm (MD5), SA Life Time (Seconds) (28800), Encapsulation (Tunnel), Perfect Forward Secrecy (PFS) (NONE), Enable Replay Detection (NO), Protocol (0), Local Port (Start: 0, End: 0), and Remote Port (Start: 0, End: 0). At the bottom right, there are 'Apply' and 'Cancel' buttons.

Phase 1	
Negotiation Mode	Main
Encryption Algorithm	DES
Authentication Algorithm	MD5
SA Life Time (Seconds)	28800
Key Group	DH1

Phase 2	
Active Protocol	ESP
Encryption Algorithm	DES
Authentication Algorithm	MD5
SA Life Time (Seconds)	28800
Encapsulation	Tunnel
Perfect Forward Secrecy(PFS)	NONE
Enable Replay Detection	NO
Protocol	0
Local Port	
Start	0
End	0
Remote Port	
Start	0
End	0

2 Setup Cisco

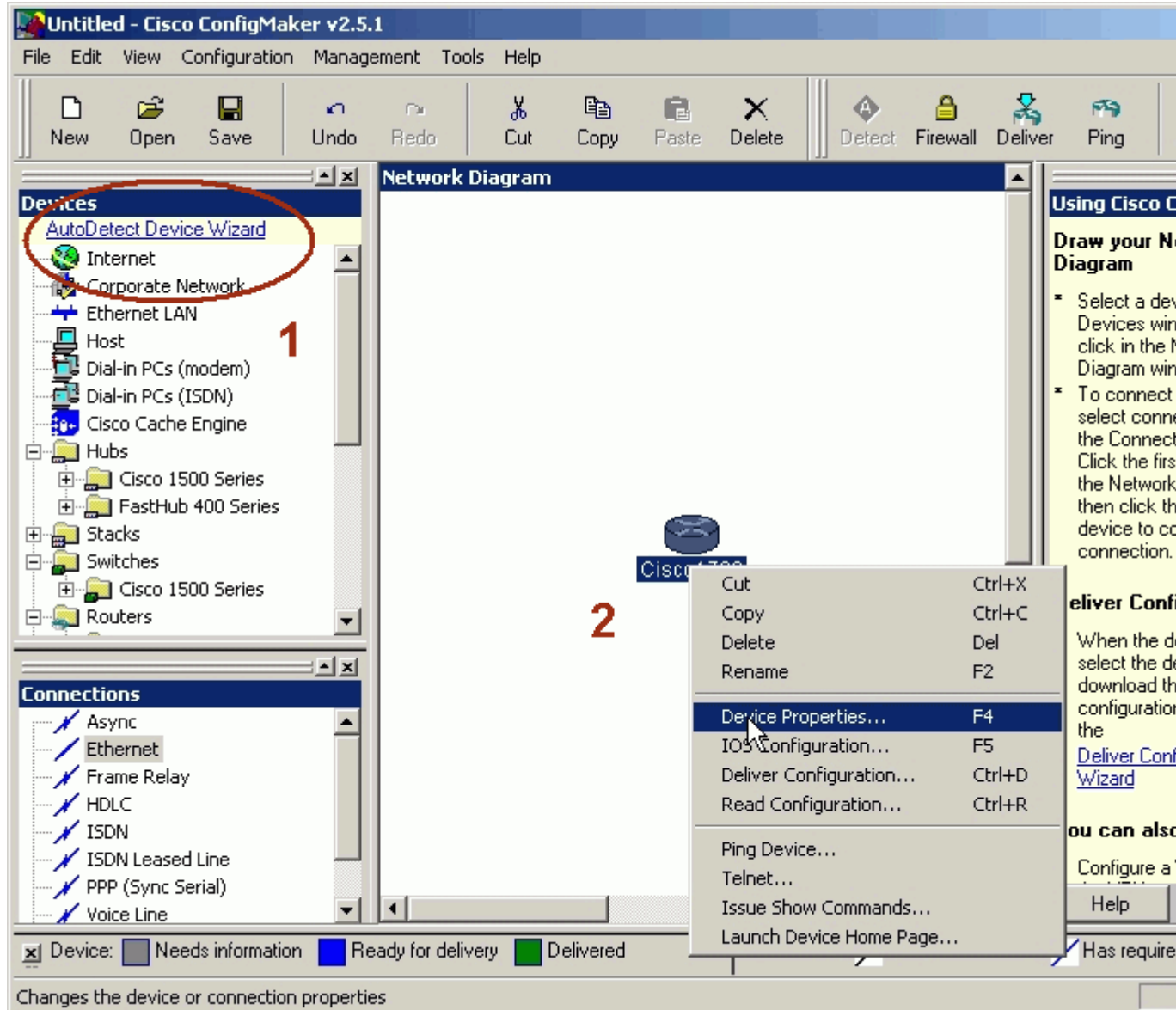
There are two ways to configure Cisco VPN, use commands from console or use **Cisco ConfigMaker**. Cisco ConfigMaker is an easy-to-use Windows 98/Me/NT/2000 application that configures Cisco routers, switches, hubs, and other devices. We will guide you how to setup IPSec by using Cisco ConfigMaker in section 2.1. If you prefer to use commands from console, please go to [section 2.2](#).

2.1 Setup Cisco by ConfigMaker

You can download Cisco ConfigMaker from <http://www.cisco.com/warp/public/cc/pd/nemns/cm/index.shtml>.

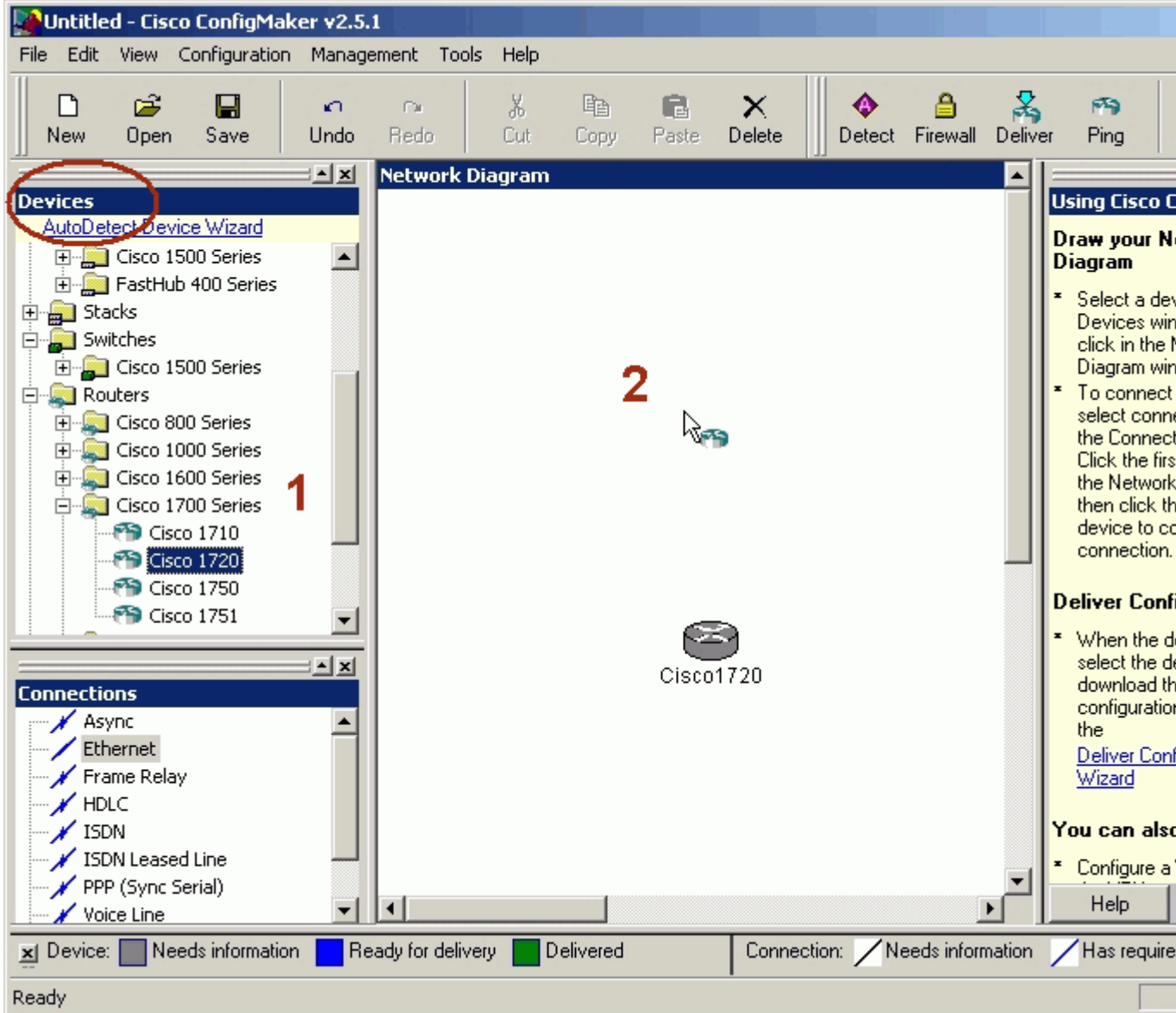
1. Select **AutoDetect device Wizard** in **Devices** window.
2. Make sure that the console has been connected to your PC. If the router is detected successfully, a Cisco router should appear in the Network Diagram Window.
3. Click right button of the mouse, choose **Device Properties...** In **Passwords** tab, setup the passwords for this router.

See the screen shot:



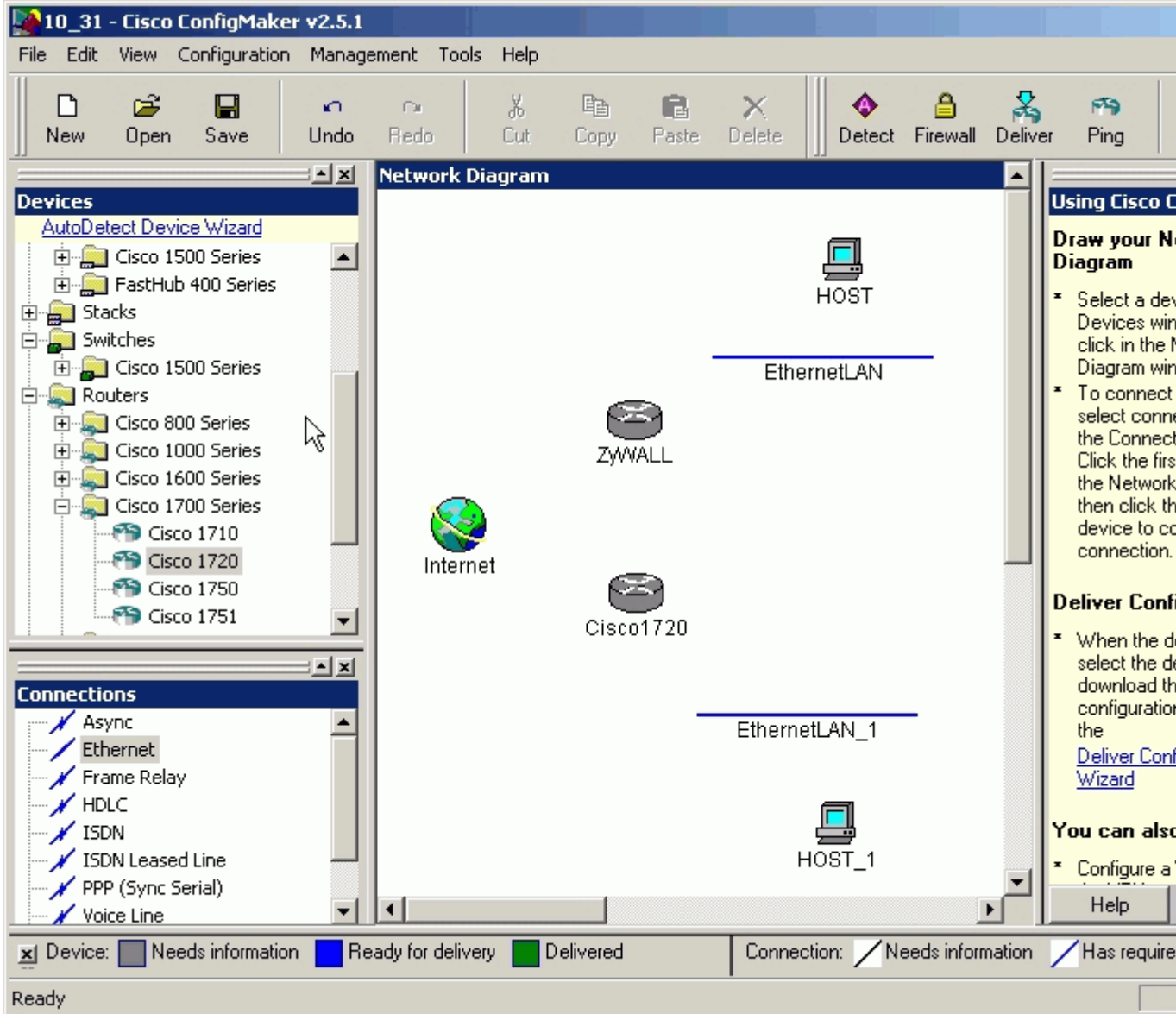
4. From **Devices window** choose a router, and add this router in **Network Diagram**. Rename it as "**ZyWALL**". Assign passwords, choose **TCP/IP** as it's protocol, and then set the interface of WAN slot 0 as **1 Ethernet**.

See the screen shot:



5. Layout your network topology in the Network Diagram as shown below. You may choose network components, such as **hosts**, **Internet**, **Ethernet LAN** from the **Devices** window.

See the screen shot:



6. Connect the network components by **Ethernet** from the **Connections** window in the left bottom. Specify the WAN and LAN IP addresses to ZyWALL and Cisco.

See the screen shot:

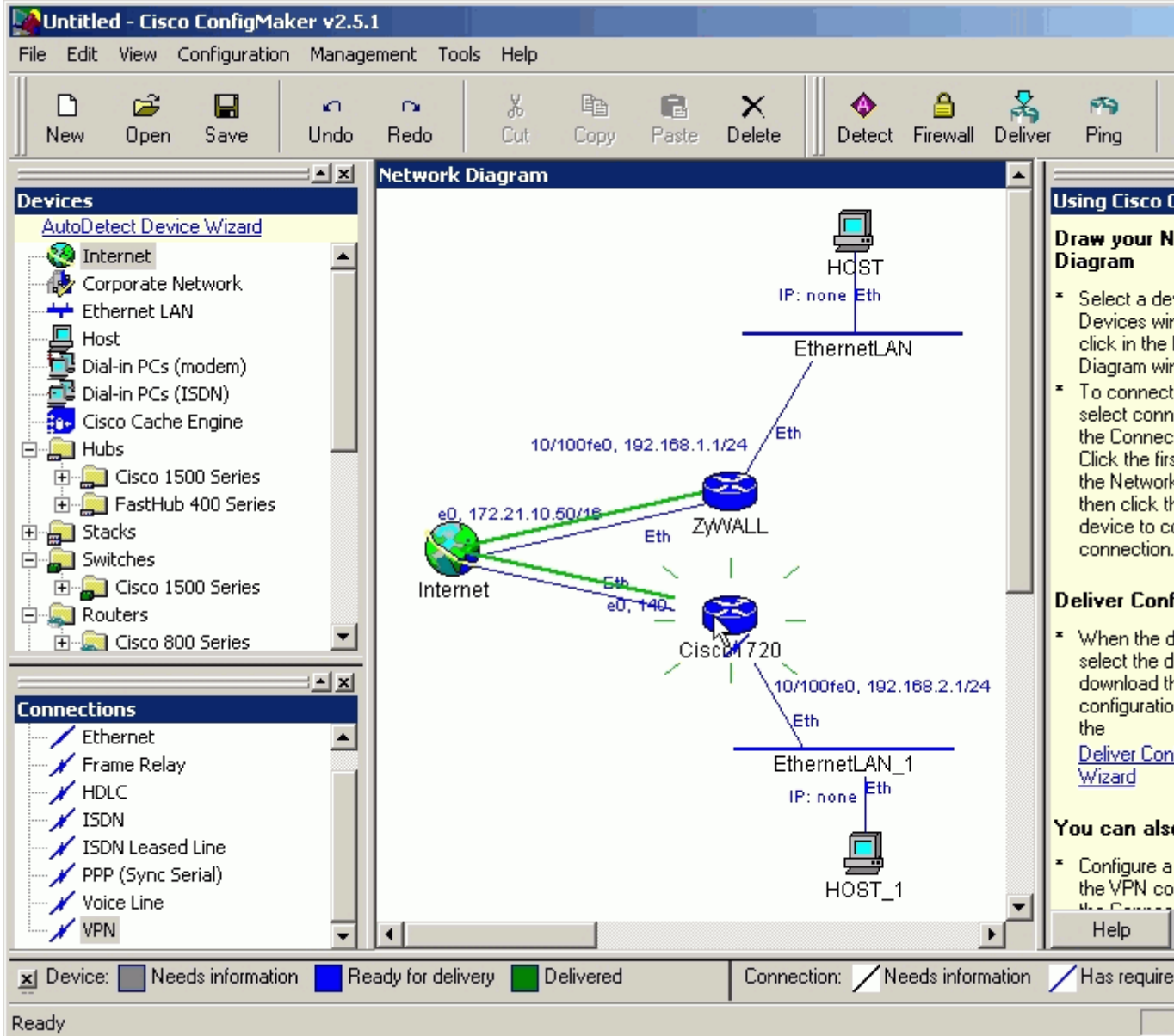
The screenshot displays the Cisco ConfigMaker v2.5.1 interface. The main window shows a network diagram with the following components and connections:

- Internet:** Represented by a globe icon with IP addresses `e0, 172.21.10.50/16` and `e0, 140.113.10.50/16`.
- ZyWALL:** A firewall device connected to the Internet and the top Ethernet LAN.
- Cisco 1720:** A router connected to the Internet and the bottom Ethernet LAN.
- EthernetLAN:** A network segment with a host icon labeled `HOST` and `IP: none`, connected to the ZyWALL.
- EthernetLAN_1:** A network segment with a host icon labeled `HOST_1` and `IP: none`, connected to the Cisco 1720.

The **Devices** window on the left lists various Cisco routers, including the Cisco 1720. The **Connections** window at the bottom left shows the **VPN** connection type selected. The status bar at the bottom indicates the device status: `Device: Needs information` (grey), `Ready for delivery` (blue), and `Delivered` (green). The connection status is `Needs information` (grey) and `Has required` (blue).

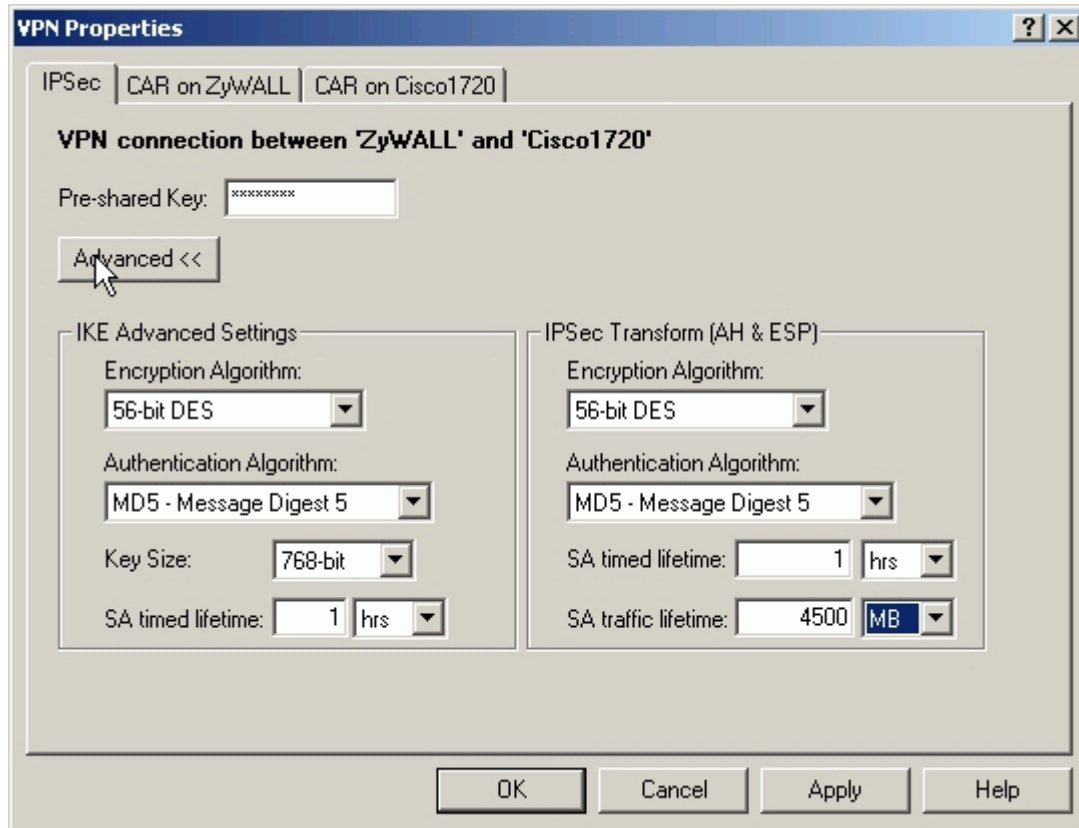
7. Select **VPN** from **Connections** window. During this stage, you have to enter the pre-shared key, "12345678".

See the screen shot:



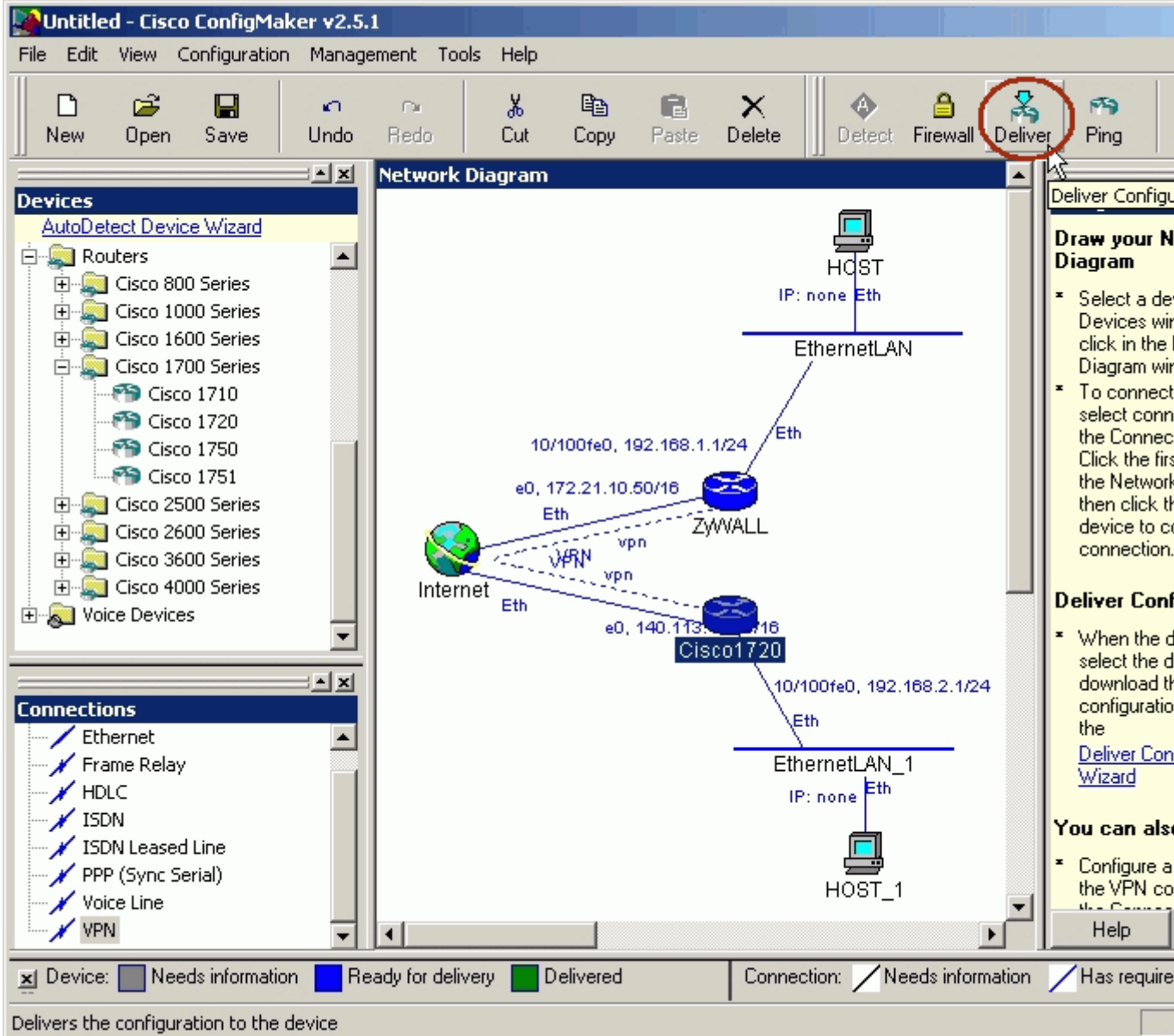
8. Select **VPN**, then click the right button of the mouse, and choose **connection Properties....** Setup IPsec parameters as shown below. Note that the parameters you set here should match settings in ZyWALL. In **IKE Advanced Settings**, **Encryption Algorithm** is **56-bit DES**, **Authentication Algorithm** is **MD5** and the **SA lifetime** is **1 hr**. In IPsec Transform, **Encryption Algorithm** is **56-bit DES**, **Authentication Algorithm** is **MD5**, and **SA lifetime** is **1 hr**.

See the screen shot:



9. Choose the Cisco router, and click **Deliver** to save the settings.

See the screen shot:



10. Enter Cisco **commands mode** from console and check if Cisco can make a successful ping to ZyWALL. You might have to tune the configuration to accommodate your practical environment. For more detailed information, please go to <http://www.cisco.com>.
11. In **config mode**, enter a command "**crypto ipsec transform-set cm-transformset-1 esp-des esp-md5-hmac**".
12. After all of the settings, if PC1 and PC2 can reach each other, then IPsec VPN has been established successfully. There is also an useful command to debug IPsec VPN, "**debug crypto ipsec**".

2.2 Setup Cisco by Commands

Note that, in order to setup Cisco by commands, you have to connect your PC and Cisco route by a console cable. Enter the following commands one per line.

Cisco1720#**config**

Cisco1720#<start typing the commands below>

```
!  
version 12.2  
no parser cache  
no service single-slot-reload-enable  
service timestamps debug uptime  
service timestamps log uptime  
service password-encryption  
!  
hostname Cisco1720  
!  
logging rate-limit console 10 except errors  
enable password 7 1543595F50  
!  
memory-size iomem 15  
mmi polling-interval 60  
no mmi auto-configure  
no mmi pvc  
mmi snmp-timeout 180  
ip subnet-zero  
!  
!  
no ip domain-lookup  
!  
ip dhcp pool 1  
    network 192.168.2.0 255.255.255.0  
    default-router 192.168.2.1  
!  
ip audit notify log  
ip audit po max-events 100  
ip ssh time-out 120  
ip ssh authentication-retries 3  
no ip dhcp-client network-discovery  
!  
crypto isakmp policy 1  
    hash md5  
    authentication pre-share  
    lifetime 3600  
crypto isakmp key 12345678 address 172.21.10.50  
!  
!  
crypto ipsec transform-set cm-transformset-1 esp-des esp-md5-hmac  
crypto mib ipsec flowmib history tunnel size 200  
crypto mib ipsec flowmib history failure size 200  
!  
crypto map cm-cryptomap local-address Ethernet0  
crypto map cm-cryptomap 1 ipsec-isakmp  
    set peer 172.21.10.50  
    set transform-set cm-transformset-1  
    match address 100  
!  
!  
!  
!
```

```

interface Ethernet0
  description connected to Internet
  ip address 140.113.10.50 255.255.0.0
  half-duplex
  crypto map cm-cryptomap
!
interface FastEthernet0
  description connected to EthernetLAN_1
  ip address 192.168.2.1 255.255.255.0
  speed auto
!
router rip
  version 1
  passive-interface Ethernet0
  network 140.113.0.0
  network 192.168.2.0
  no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0
no ip http server
!
access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
!
!
snmp-server community public RO
!
line con 0
  exec-timeout 0 0
  password 7 06575D7218
  login
line aux 0
line vty 0 4
  password 7 11584B5643
  login
line vty 5 15
  login
!
no scheduler allocate
end

```

After all of the settings, if PC1 and PC2 can reach each other, then IPsec VPN has been established successfully. There is also a useful command to debug IPsec VPN, "**debug crypto ipsec**".