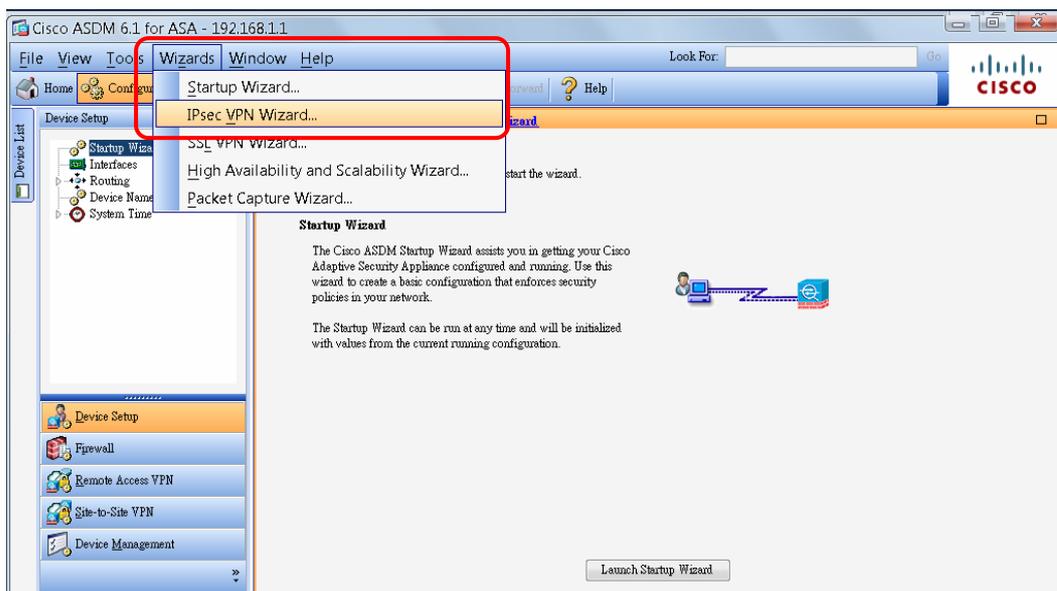


How to build LAN to LAN VPN connection between Vigor router and CiscoASA

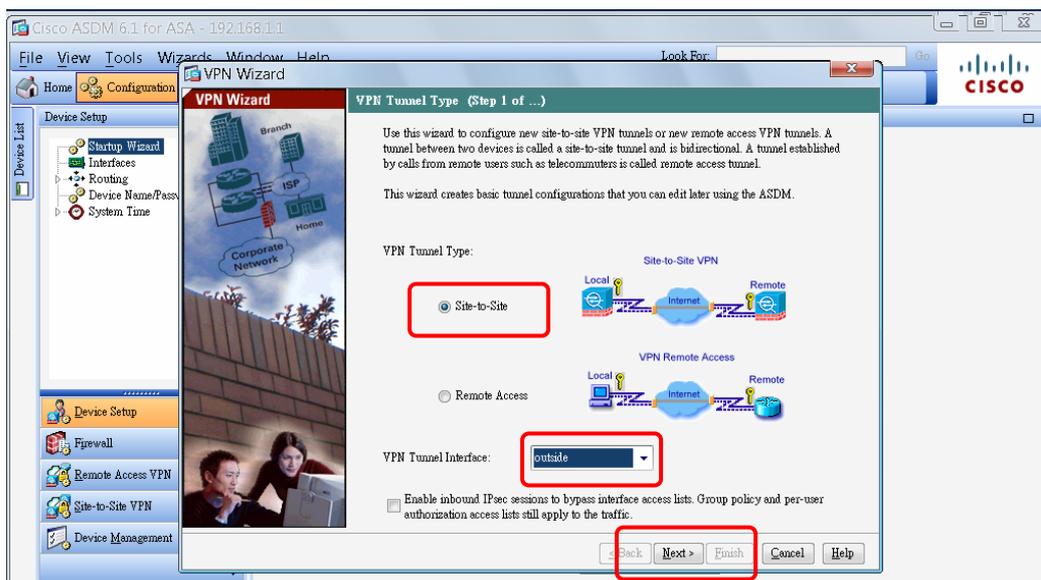
This application will guide you to build LAN to LAN VPN connection between Vigor router (e.g., Vigor2910) and CiscoASA. Suppose,

- The WAN IP address of CISCO ASA is 203.70.63.90, while LAN IP address is 192.168.1.1/255.255.255.0
- The WAN1 IP address of Vigor2910 is 59.125.9.159; while LAN IP is 192.169.20.1/255.255.255.0

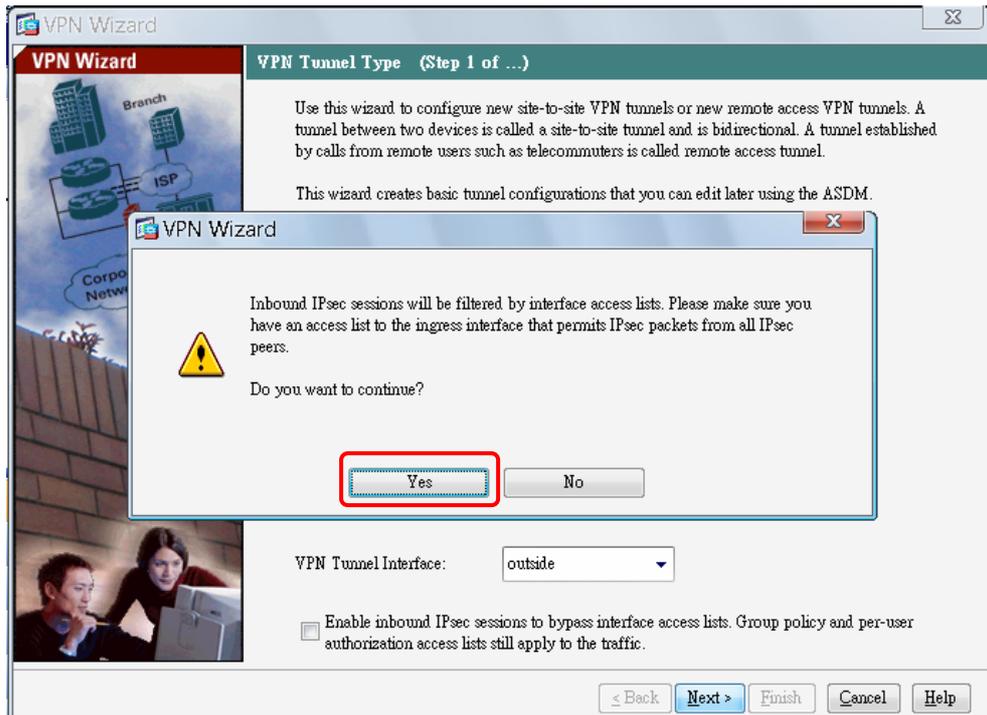
1. Choose **Wizards>>IPsec VPN Wizard**.



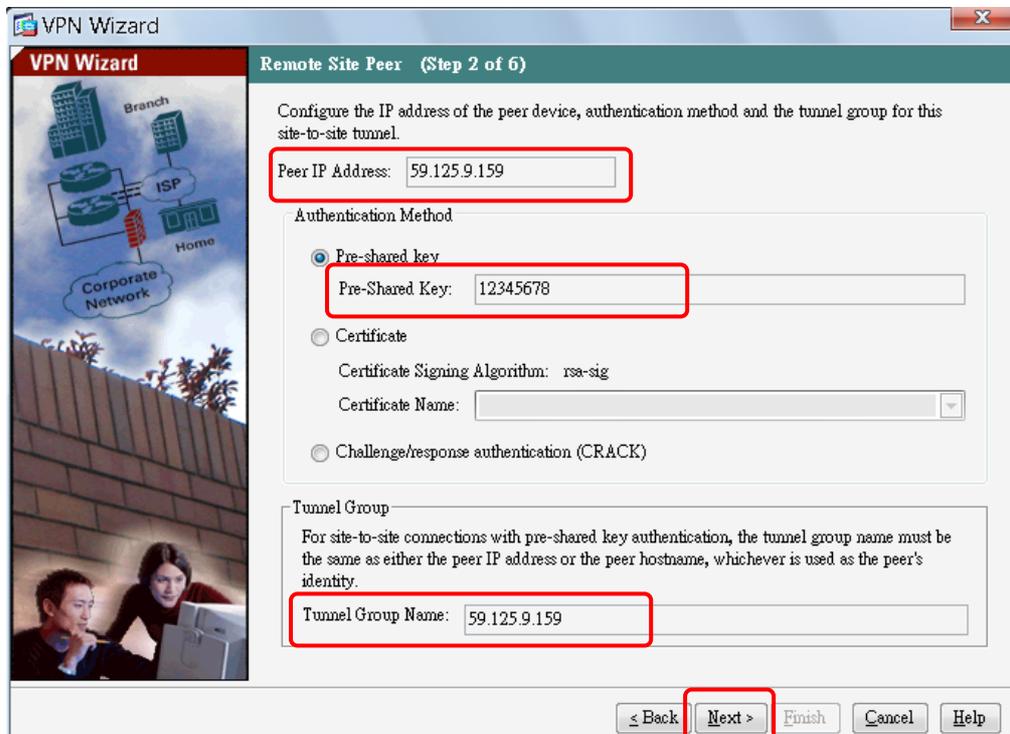
2. The VPN Wizard will be popped-up as follows. Choose **Site-to-Site** as **VPN Tunnel Type**; **Outside** as **VPN Tunnel Interface**; and click **Next**.



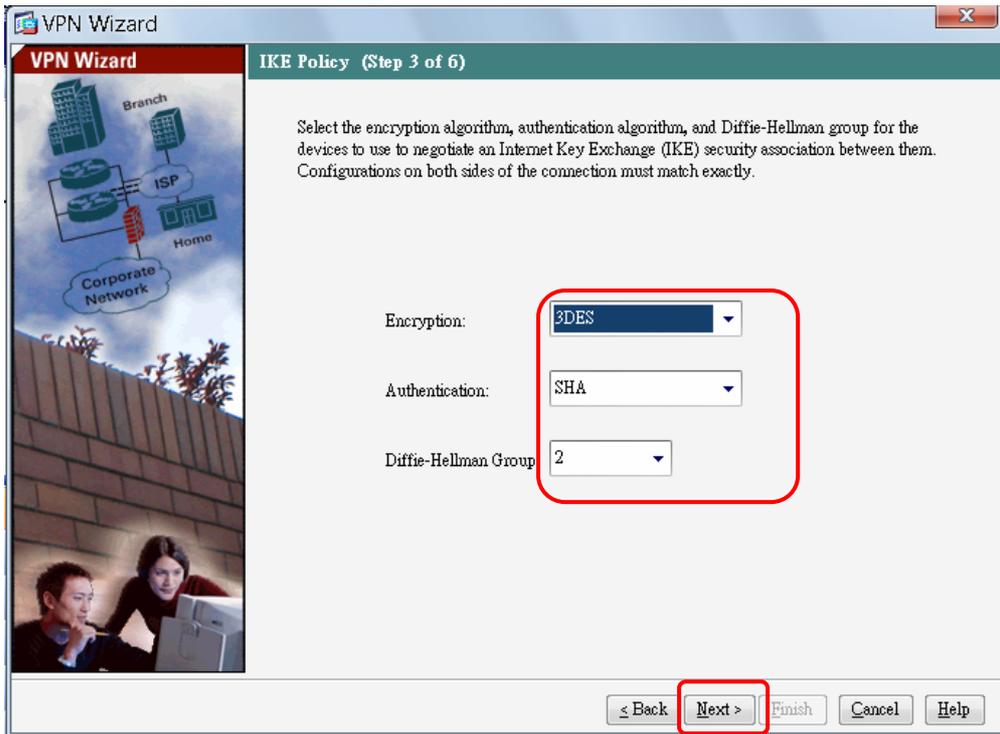
3. Click **Yes** to continue.



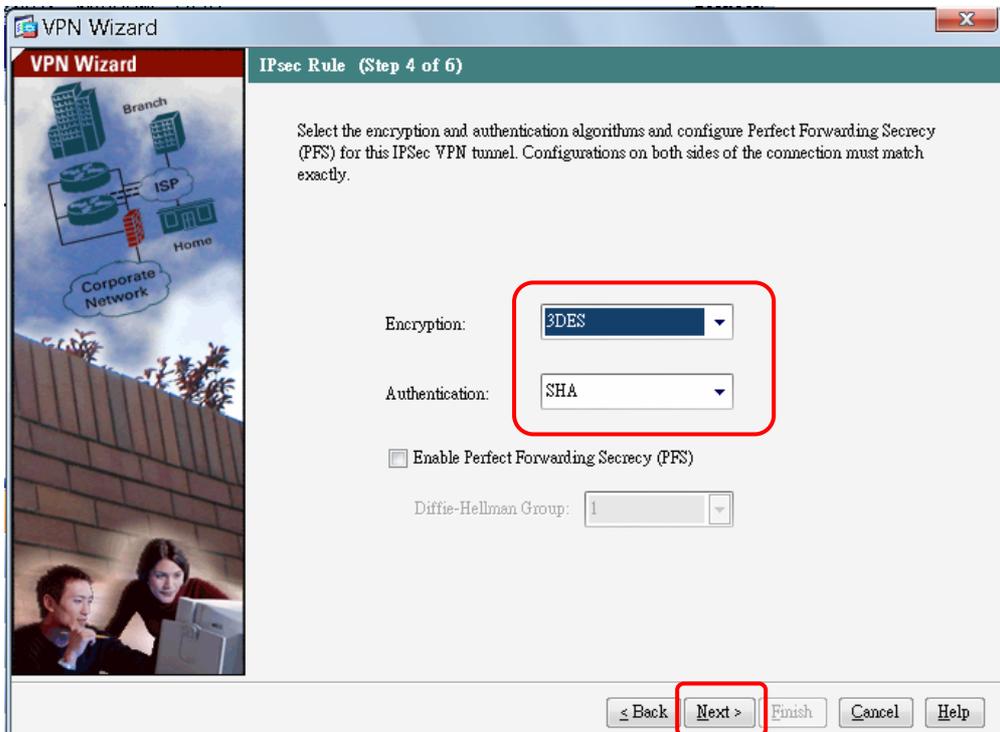
4. Type the WAN IP address of the peer in the field of **Peer IP Address** for IPsec VPN connection. Then type the Pre-shared key. Next, a profile name will be generated automatically in the field of **Tunnel Group Name**. Click **Next**.



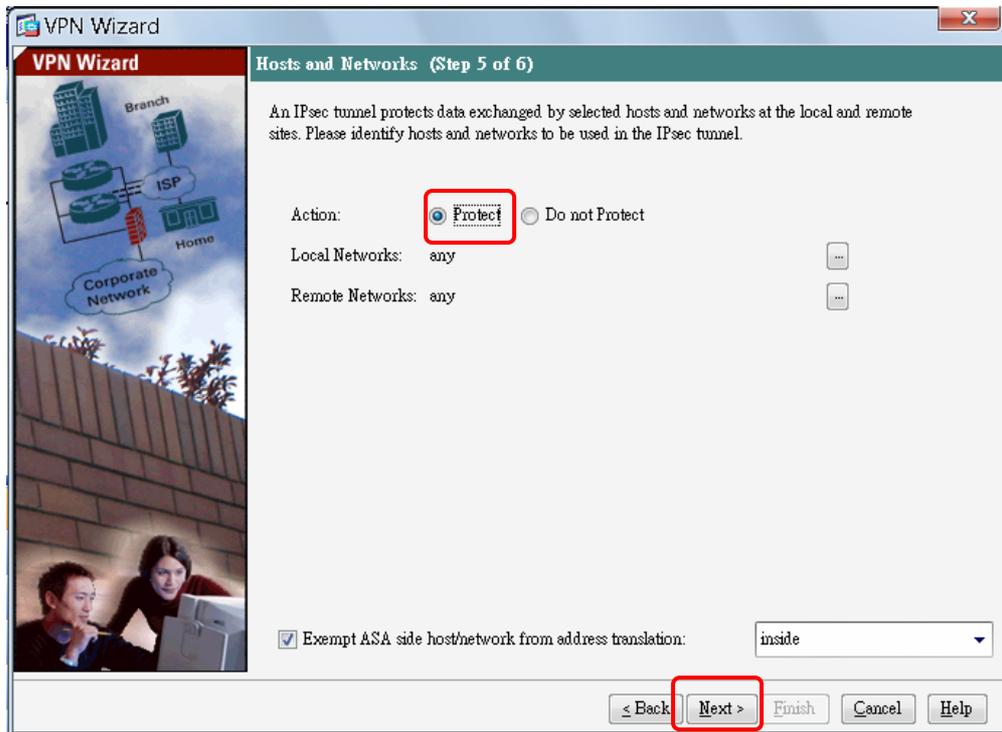
5. Keep the default settings of **Encryption** type and **Authentication**, and specify the **DH Group** for your request. Then, click **Next**.



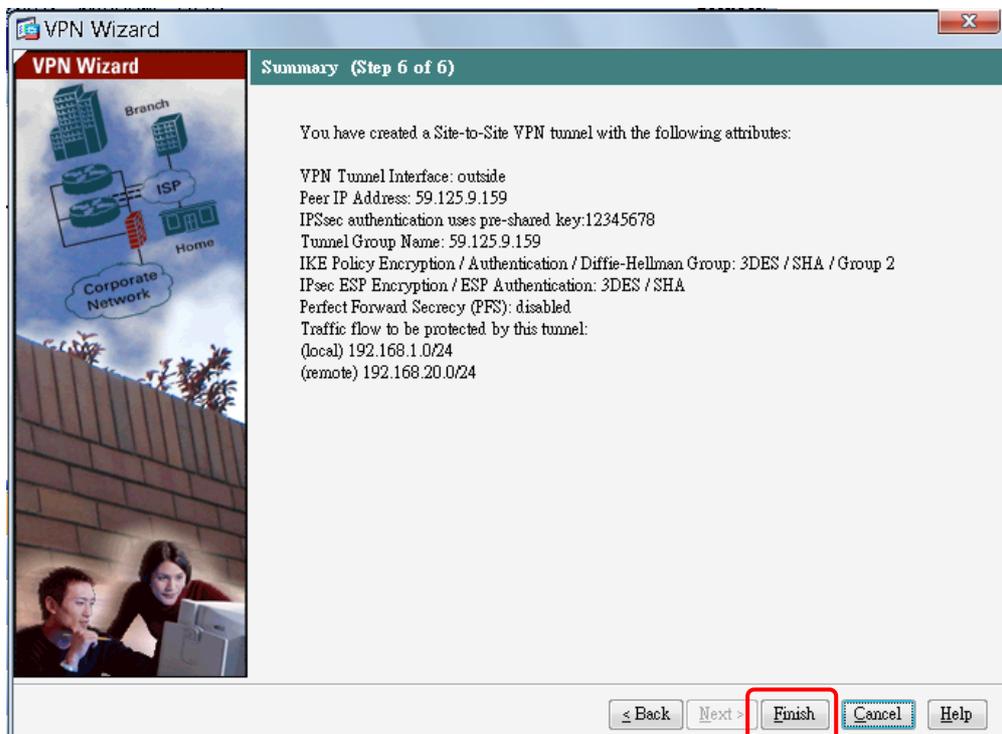
6. For the second phase of IKE encryption, keep the default settings and click **Next**.



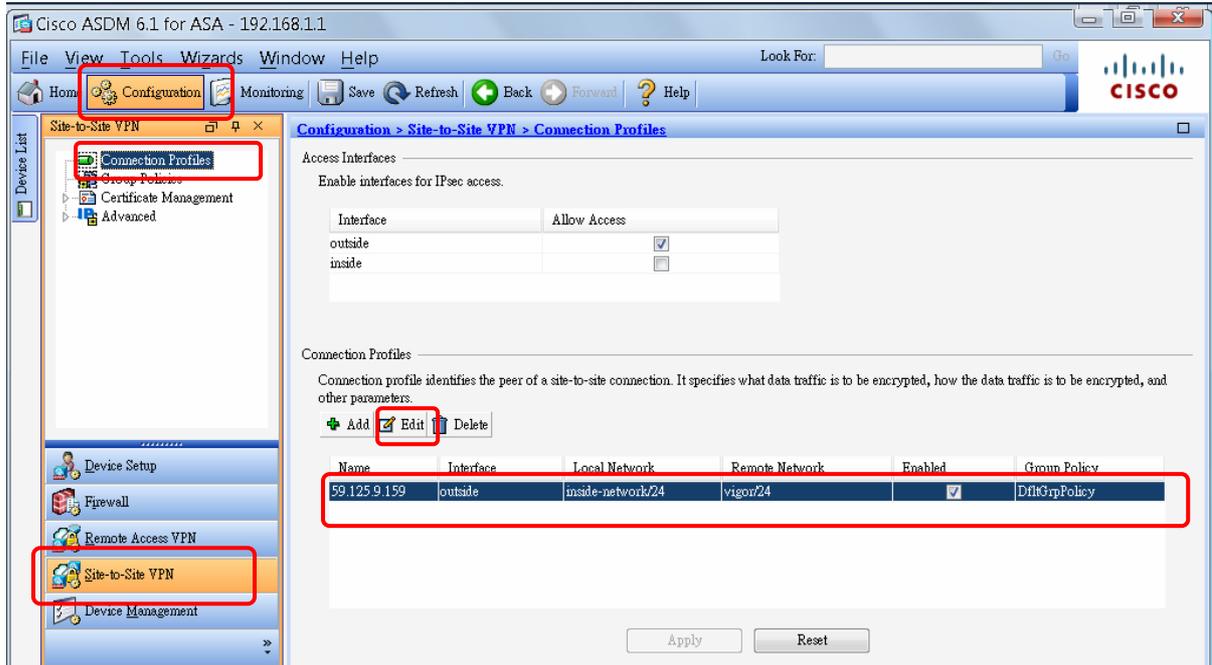
7. In the following screen, type the local / remote IP address with the subnet mask for local /remote network. Then, click **Next**.



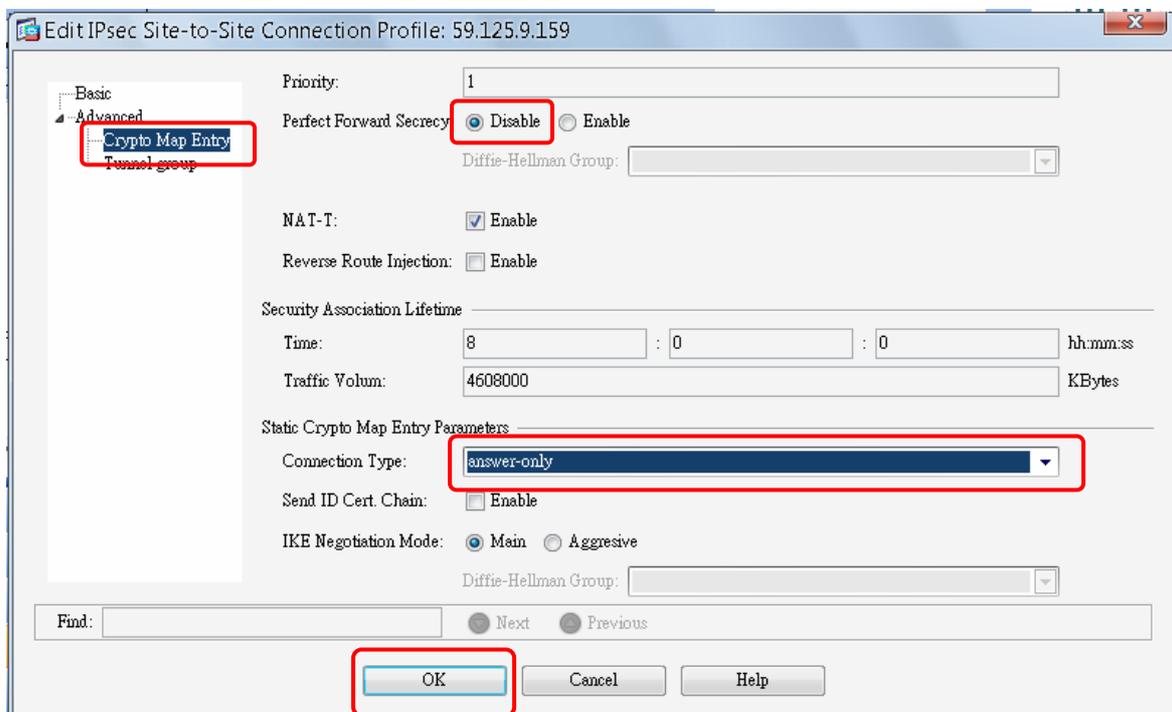
8. Click **Finish**.



- Click the tab of **Configuration**. Choose **Site-to-Site VPN** and click **Connection Profiles**. Now, the relational VPN settings will be displayed on the field of **Connection Profiles**. If required, you can click **Edit** on this field to modify other settings of VPN in details.

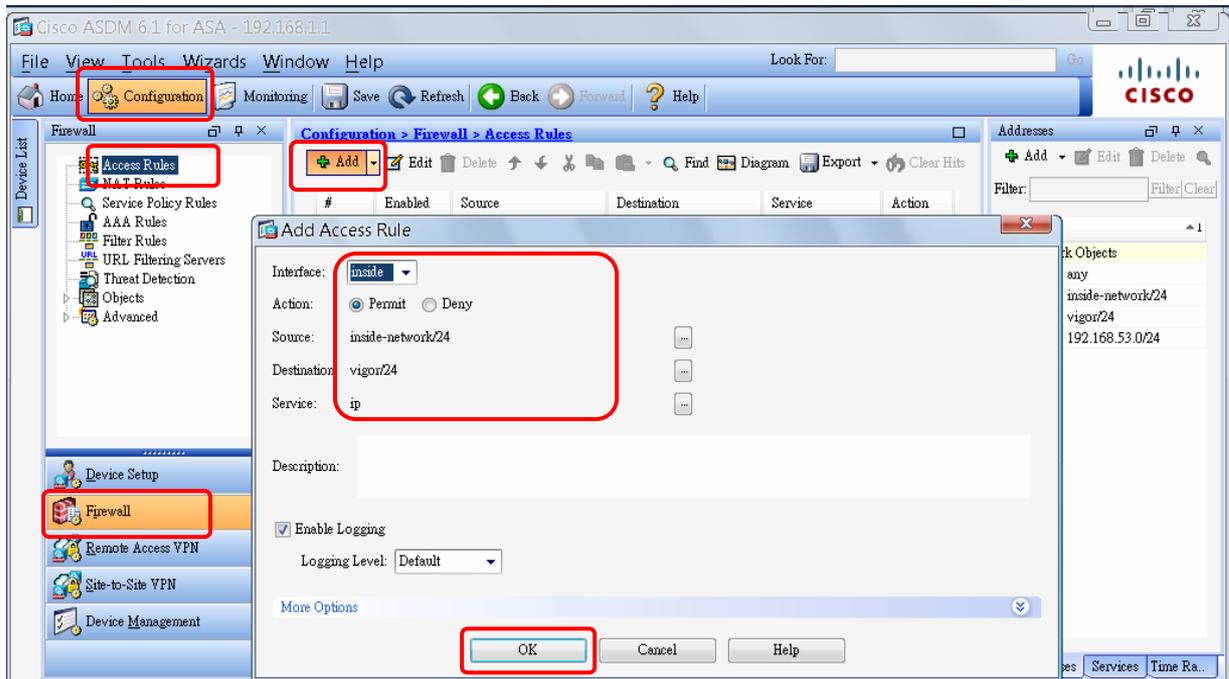


- Click **Edit** to open the following screen. Expand the **Advanced** folder and choose **Crypto Map Entry**. Click **Disable** for **Perfect Forward Secrecy**, then choose **answer-only** as **Connection Type**. Next, click **OK**.

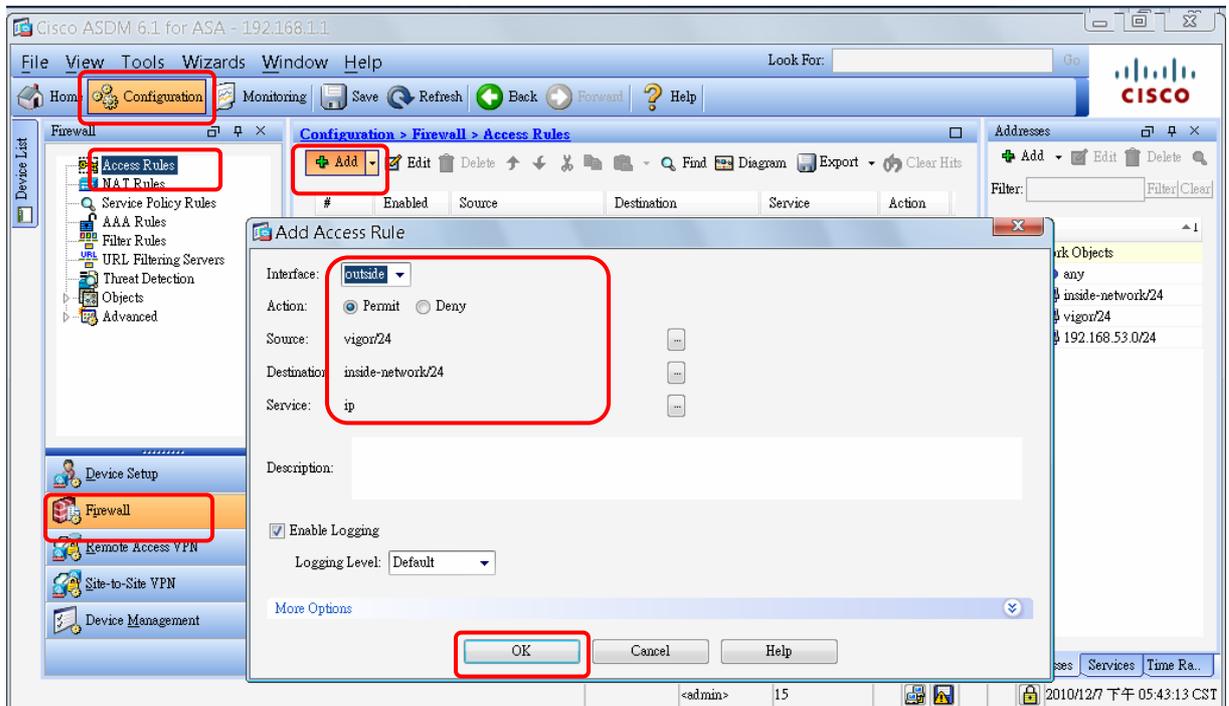


- Click the tab of **Configuration**. Choose **Firewall** and click **Access Rules**.

12. Click **Add**. The **Add Access Rule** dialog will pop-up. Choose **Inside** as the **Interface**; and choose **Permit** as the **Action**. Choose local network as the **Source**; and remote network as the **Destination**. Next, click **OK**.



13. Click **Add** to add another access rule. Choose **Outside** as the **Interface**; and choose **Permit** as the **Action**. Choose remote network as the **Source**; and local network as the **Destination**. Next, click **OK**.



14. Access into the WUI of Vigor router (e.g., Vigor2910).

15. Open **VPN and Remote Access>>LAN to LAN**. Click index #1.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles: | [Set to Factory Default](#) |

Index	Name	Status	Index	Name	Status
<u>1.</u>	2.29	X	<u>17.</u>	???	X
<u>2.</u>	2.229	X	<u>18.</u>	???	X
<u>3.</u>	24	X	<u>19.</u>	???	X
<u>4.</u>	25	X	<u>20.</u>	???	X
<u>5.</u>	26	X	<u>21.</u>	???	X
<u>6.</u>	27	X	<u>22.</u>	???	X
<u>7.</u>	28	X	<u>23.</u>	???	X
<u>8.</u>	29	X	<u>24.</u>	???	X
<u>9.</u>	30	X	<u>25.</u>	???	X
<u>10.</u>	???	X	<u>26.</u>	???	X
<u>11.</u>	???	X	<u>27.</u>	???	X
<u>12.</u>	???	X	<u>28.</u>	???	X
<u>13.</u>	???	X	<u>29.</u>	???	X
<u>14.</u>	???	X	<u>30.</u>	???	X
<u>15.</u>	???	X	<u>31.</u>	???	X
<u>16.</u>	???	X	<u>32.</u>	???	X

[XXXXXXXX:This Dial-Out Profile has already joined for VPN BACKUP Mechanism]
 [XXXXXXXX:This Dial-Out Profile does not join for VPN TRUNK]

16. Type a name for such profile (e.g, cisco, in this case) and check the box of **Enable this profile**. Click **Dial-Out** as **Call Direction** and check **Always on**. Next, choose **IPSec Tunnel** as the **Type of Server I am calling**. Type the WAN IP address of the Peer (e.g., 203.70.63.90, in this case). Specify a Pre-Shared Key which must be the same as the settings configured in ASA.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

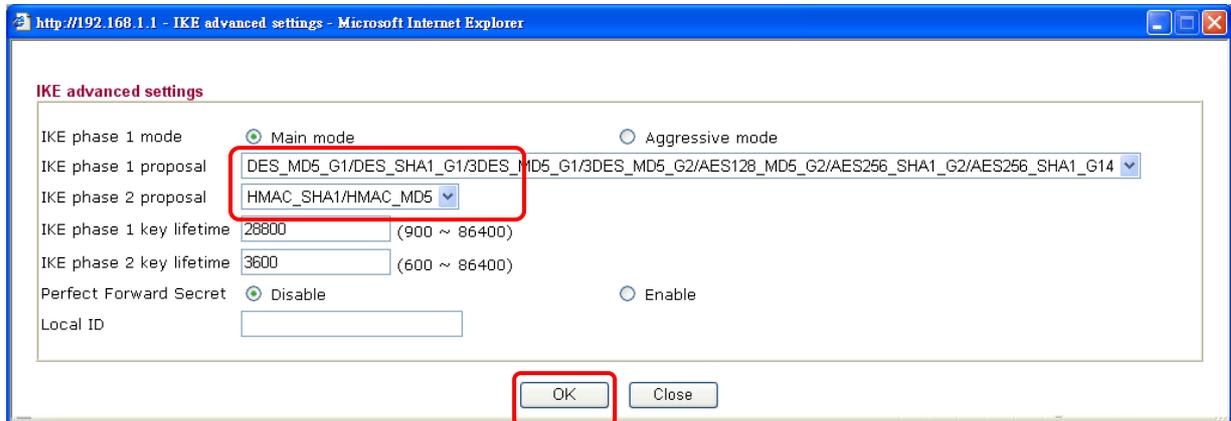
1. Common Settings

Profile Name: <input type="text" value="cisco"/>	Call Direction: <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-In
<input checked="" type="checkbox"/> Enable this profile	<input checked="" type="checkbox"/> Always on
VPN Connection Through: <input type="text" value="WAN1 First"/>	Idle Timeout: <input type="text" value="300"/> second(s)
Netbios Naming Packet: <input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep alive
Multicast via VPN: <input type="radio"/> Pass <input checked="" type="radio"/> Block <small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small>	PING to the IP: <input type="text"/>

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPSec Tunnel <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/>	Link Type: <input type="text" value="64k bps"/>
Dial Number for ISDN or Server IP/Host Name for VPN. <small>(such as 5551234, draytek.com or 123.45.67.89)</small> <input type="text" value="203.70.63.90"/>	Username: <input type="text" value="???"/> Password: <input type="text"/> PPP Authentication: <input type="text" value="PAP/CHAP"/> VJ Compression: <input checked="" type="radio"/> On <input type="radio"/> Off
	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key: <input type="text" value="●●●●●●"/> <input type="radio"/> Digital Signature(X.509) <input type="text" value="None"/>

17. As for **IPSec Security Method**, choose **High**. Click **Advanced** to open **IKE advanced settings** dialog box. In the dialog, please choose the **IKE phase 1 proposal** and **IKE phase 2 proposal** settings based on the network environment. Next, click **OK** to save the settings and exit the dialog.



18. Type the remote network IP address and subnet mask (e.g., the inside interface of CiscoASA). Then, click **OK**.

4. GRE over IPSec Settings

Enable IPSec Dial-Out function GRE over IPSec

Logical Traffic My GRE IP Peer GRE IP

5. TCP/IP Network Settings

My WAN IP	<input type="text" value="0.0.0.0"/>	RIP Direction	<input type="text" value="Disable"/>
Remote Gateway IP	<input type="text" value="0.0.0.0"/>	From first subnet to remote network, you have to do	
Remote Network IP	<input type="text" value="192.168.1.0"/>	<input type="text" value="Route"/>	
Remote Network Mask	<input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network IP	<input type="text" value="192.168.20.1"/>		
Local Network Mask	<input type="text" value="255.255.255.1"/>		

19. Now, a LAN to LAN VPN connection between Vigor router and CiscoASA has been established.