

VPN Configuration Using Cisco Packet Tracer

Abstract:

A private network is a reliable way of communicating with various units and communicating with internal networks. Internet Protocol Security (IPsec) Virtual Private Network (VPN) is one of the most powerful security tool , safest and most secure option available in the Private Network which is used in remote areas.

Here, the VPN Configuration is established using **isakmp** command, **ipsec** tunnels using cisco packet tracer.

Motivation / Challenge:

The main moto of this project is to connect anonymously by creating a private network from a public internet connection (Internet Router) (ie) the connection goes through a ipsec tunnel.

The challenge faced are:

- Limited no of VPN Connections based on the availability of IP Addresses.
- Takes lot of time to physically configure a new connection and requires more hardware.

To overcome this we can have connect more servers and modern routers which can support many devices in both wired and wireless configurations.

Objective:

VPN Configuration (Remote Access) using Cisco Packet Tracer.

Software / Hardware requirements:

Cisco Packet Tracer – Version 8.0.0.0212

Engineering Standards:

A virtual private network (VPN) can be defined as a way to provide secure communication between members of a group through use of public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. There are many different VPN solutions out there, and just deciding which one to choose can be difficult since they all have advantages and disadvantages. VPNs can be categorized as Secure or Trusted VPNs, Client-based or Web-based VPNs and Provider Edge-based VPNs.

Realistic Constraint:

This model is only suitable for limited number of PCs, if overloaded, the server might malfunction, connection may drop and the anonymity will be lost.

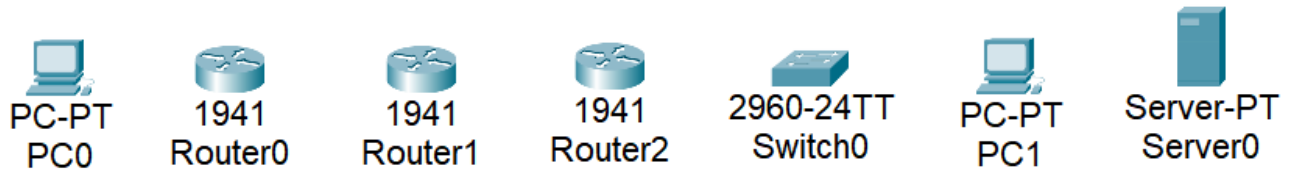
Deliverables:

1. Remote Access
2. Secure Network
3. Anonymity

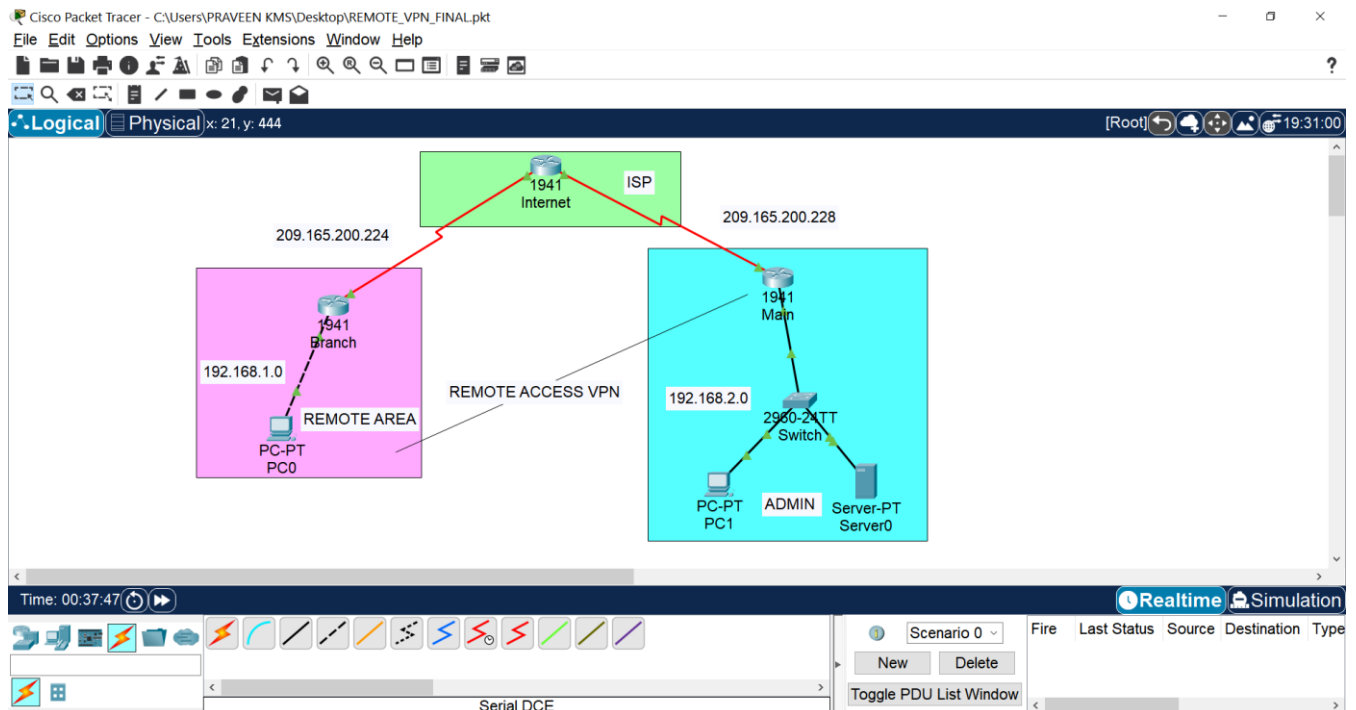
Methodology:

- **Schematic Diagram:**

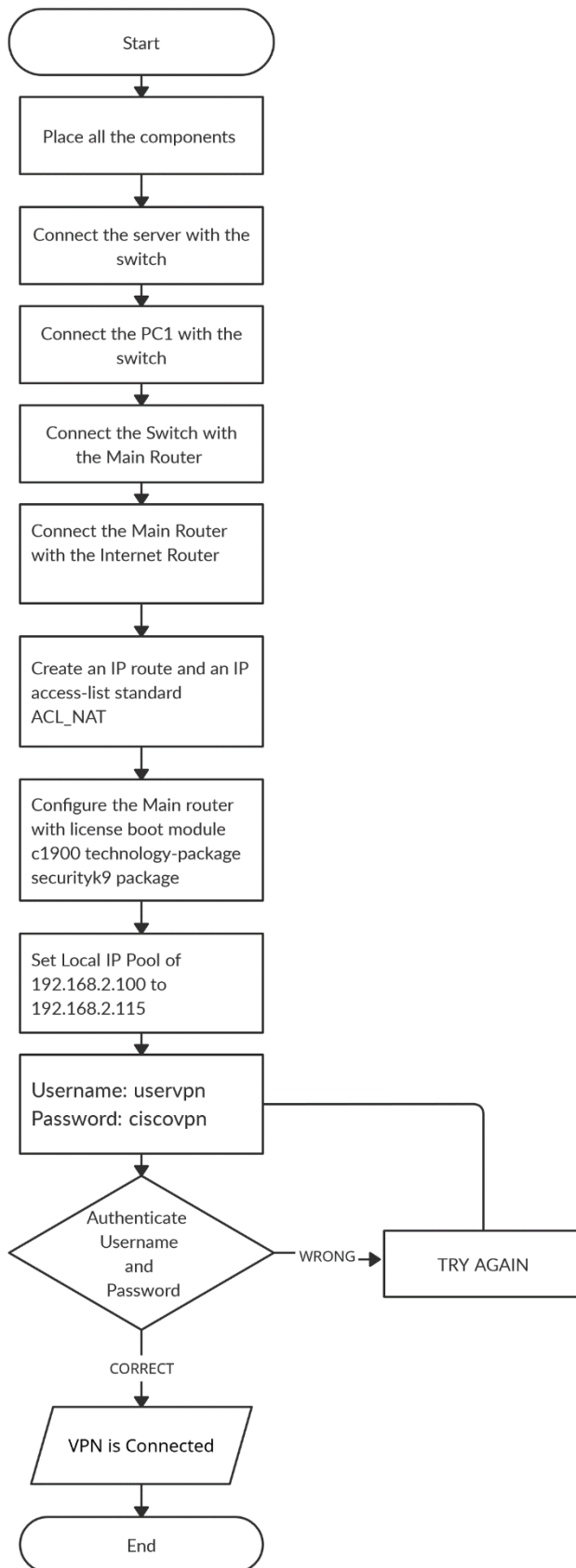
1. Components Used:



2. Final Schematic:



- **Flowchart:**



- **Algorithm :**

Step 1: Place 3 Routers(1941),2 PCs,1 Switch,1 Server in the framework.

Step 2: Connect the server with the switch and the IP address 192.168.2.254 is assigned to the server.

Step 3: Connect the PC1 with the switch with IP address 192.168.2.10.

Step 4: Connect the Switch with the Main Router with IP address 192.168.2.1

Step 5: Connect the Main Router with the Internet Router with Serial DCE(s0/0/1) cable with the IP 209.165.200.229

Step 6: Connect the Internet Router with the Branch Router with Serial DCE(s0/0/0) cable with IP 209.165.200.225

Step 7: Connect the Branch Router with PC0 with IP 192.168.1.10 with Fa0.

Step 8: Create an IP route 0.0.0.0 0.0.0.0 s0/0/0 in the Branch Router.

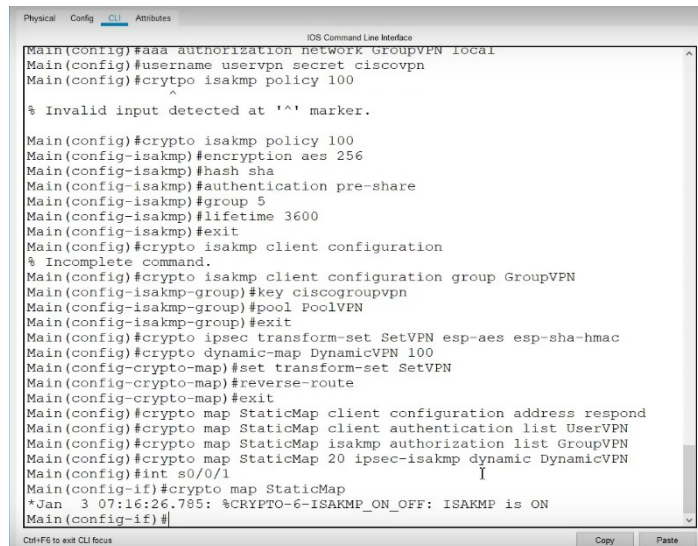
Step 9: Create an IP access-list standard ACL_NAT permitting 192.168.1.0 with inside and outside.

Step 10: Configure the Main router with **license boot module c1900 technology-package securityk9** package.

Step 11: Set Local IP Pool of 192.168.2.100 to 192.168.2.115 and set the username as uservpn

and the password ciscovpn using aaa authorization and crypto isakmp policy 100, encryption aes 256,hash sha.

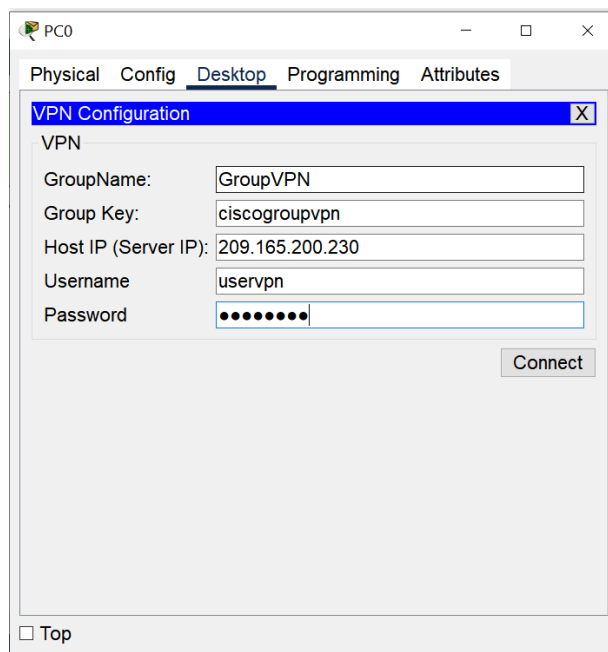
Step 12: Set the key as ciscogroupvpn :



```
Physical Config CLI Attributes
IOS Command Line Interface
Main(config)#aaa authorization network GroupVPN local
Main(config)#username uservpn secret ciscovpn
Main(config)#crypto isakmp policy 100
Main(config)#crypto isakmp policy 100
Main(config-isakmp)#encryption aes 256
Main(config-isakmp)#hash sha
Main(config-isakmp)#authentication pre-share
Main(config-isakmp)#group 5
Main(config-isakmp)#lifetime 3600
Main(config-isakmp)#exit
Main(config)#crypto isakmp client configuration
Main(config)#crypto isakmp client configuration group GroupVPN
Main(config-isakmp-group)#key ciscogroupvpn
Main(config-isakmp-group)#pool PoolVPN
Main(config-isakmp-group)#exit
Main(config)#crypto ipsec transform-set SetVPN esp-aes esp-sha-hmac
Main(config)#crypto dynamic-map DynamicVPN 100
Main(config-crypto-map)#set transform-set SetVPN
Main(config-crypto-map)#reverse-route
Main(config-crypto-map)#exit
Main(config)#crypto map StaticMap client configuration address respond
Main(config)#crypto map StaticMap client authentication list UserVPN
Main(config)#crypto map StaticMap isakmp authorization list GroupVPN
Main(config)#crypto map StaticMap 20 ipsec-isakmp dynamic DynamicVPN
Main(config)#int s0/0/1
Main(config-if)#crypto map StaticMap
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Main(config-if)#
```

(MAIN ROUTER)

Step 13: VPN DETAILS:



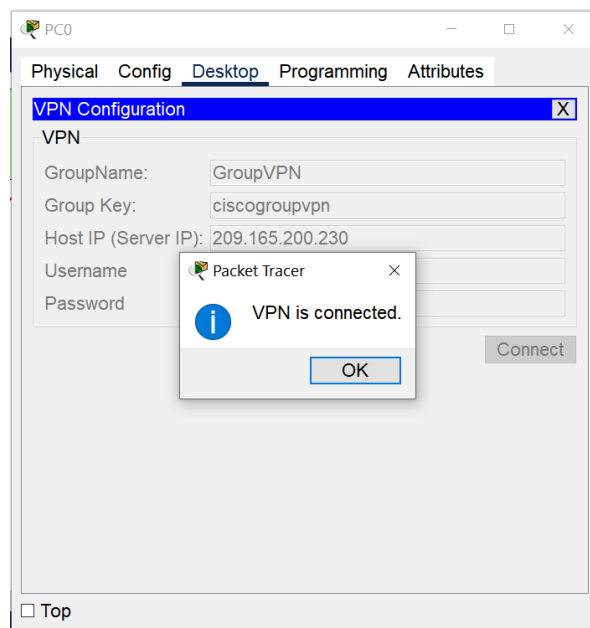
The screenshot shows the 'VPN Configuration' window in the Packet Tracer PC0 Desktop environment. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The 'VPN' section contains the following fields:

- GroupName: GroupVPN
- Group Key: ciscogroupvpn
- Host IP (Server IP): 209.165.200.230
- Username: uservpn
- Password: ciscovpn (masked with dots)

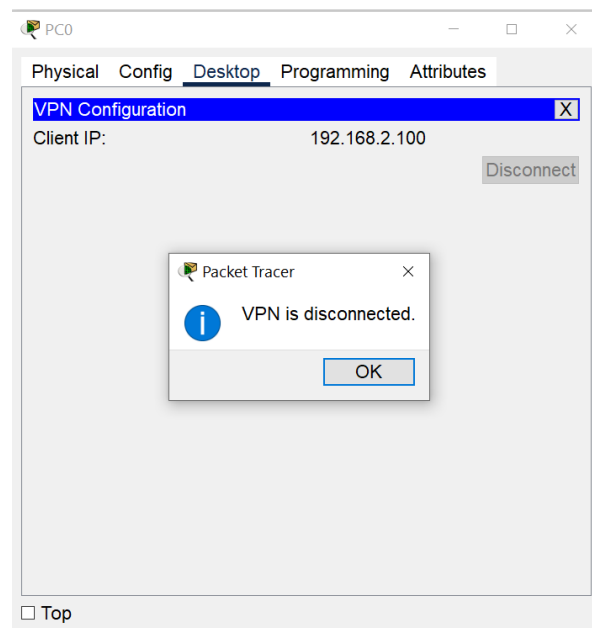
A 'Connect' button is located at the bottom right of the configuration area. A 'Top' button is at the bottom left of the window.

Password: ciscovpn

Output:



This screenshot shows the 'VPN Configuration' window with a 'Packet Tracer' dialog box overlaid. The dialog box contains an information icon and the text 'VPN is connected.' with an 'OK' button. The background configuration fields are the same as in the previous screenshot.



This screenshot shows the 'VPN Configuration' window with a 'Disconnect' button at the top right. A 'Packet Tracer' dialog box is overlaid, displaying 'VPN is disconnected.' with an 'OK' button.

(VPN Connection Status)

Verification of VPN Connection:

[illegible]

Result

The VPN using **isakmp** and **ipsec** was configured successfully using Cisco Packet Tracer.

Conclusion

This Project is about VPN and IPsec protocols. The aim of the project is to explain the service of VPN and to know about the VPN protocol (IPsec) used for safeguarding a connection. The IPsec VPN is a secure protocol to create the non-public connection at low charge. In comparison with the WAN device, the VPN is an inexpensive one. IPsec VPN can be applied on hosts and router gateways. The whole IP packet is encrypted and then authenticated in tunnel mode. Then, a new IP packet is created with which is connected and encapsulated.

References

1. Sadia Jabbar Anwar, Ibtahaj Ahmad, "Design and Deployment of IPsec VPN Using CISCO Network Infrastructure", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 6, pp.237-247, November-December 2019. Link: <https://doi.org/10.32628/CSEIT195630>
Journal URL : <http://ijsrcseit.com/CSEIT195630>
2. Murhammer, M.W., Atakan, O., Badri, Z., Cho, B., Lee, H.J. and Schmid, " A Comprehensive Guide to Virtual Private Networks", Volume III, Cross-Platform Key and Policy Management, 1999.
3. Liu D, Miller S, Lucas M, Singh A, Davis J. Firewall policies and VPN configurations. Elsevier; 2006, Sep 28
4. <https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html>
5. https://www.google.co.in/books/edition/IKEv2_IPsec_Virtual_Private_Networks/iHvSDAAQBAJ?hl=en&gbpv=0
6. <https://www.google.co.in/books/edition/VPNs/6wMoAQAAMAAJ?hl=en&gbpv=1&bsq=vpn&dq=vpn&printsec=frontcover>