Setup L2TP over IPSec Server on RV340 Series

Objective

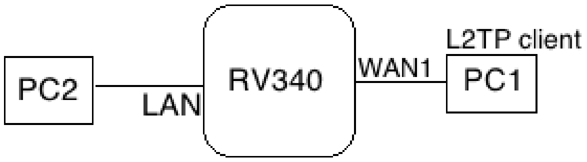
When RV340 acts as L2TP/PPTP server, we can use external radius server or local database to authenticate the users. The local database authentication only support PAP. This example describes how to setup the RV340 L2TP over IPSec server and Windows/MACOS clients.

Devices

- RV340
- WINDOWS 10

This Document will guide you how to use RV340 local database to authenticate WIN10 client (L2TP/IPsec).

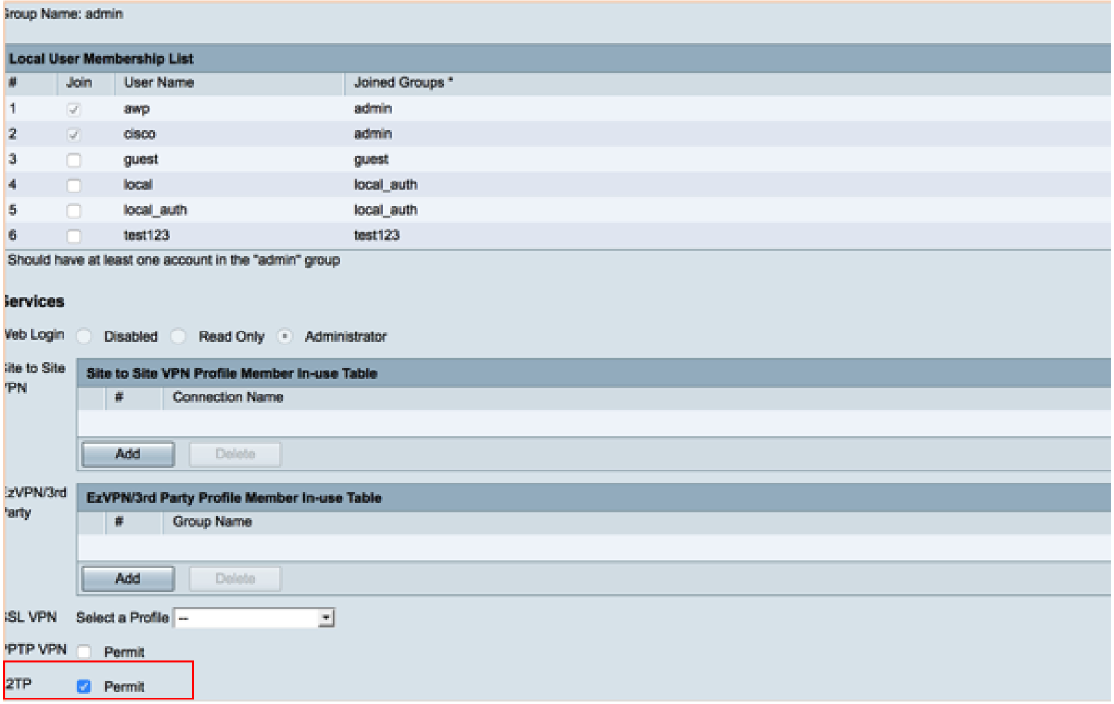
Topo



RV340 is the L2TP server. PC1 is the L2TP client. PC2 is used to manage RV340.

Steps:

Step1: configure the user&groups. Permit the L2TP service for this group. (here as example, just used the default admin group)



iroup Name: admin

Local User Membership List

#	Join	User Name	Joined Groups *
1	☑	awp	admin
2	☑	cisco	admin
3	□	guest	guest
4	□	local	local_auth
5	□	local_auth	local_auth
6	□	test123	test123

Should have at least one account in the "admin" group

iervices

Veb Login ○ Disabled ○ Read Only ● Administrator

iite to Site 'PN

Site to Site VPN Profile Member In-use Table

#	Connection Name

:zVPN/3rd 'arty

EzVPN/3rd Party Profile Member In-use Table

#	Group Name

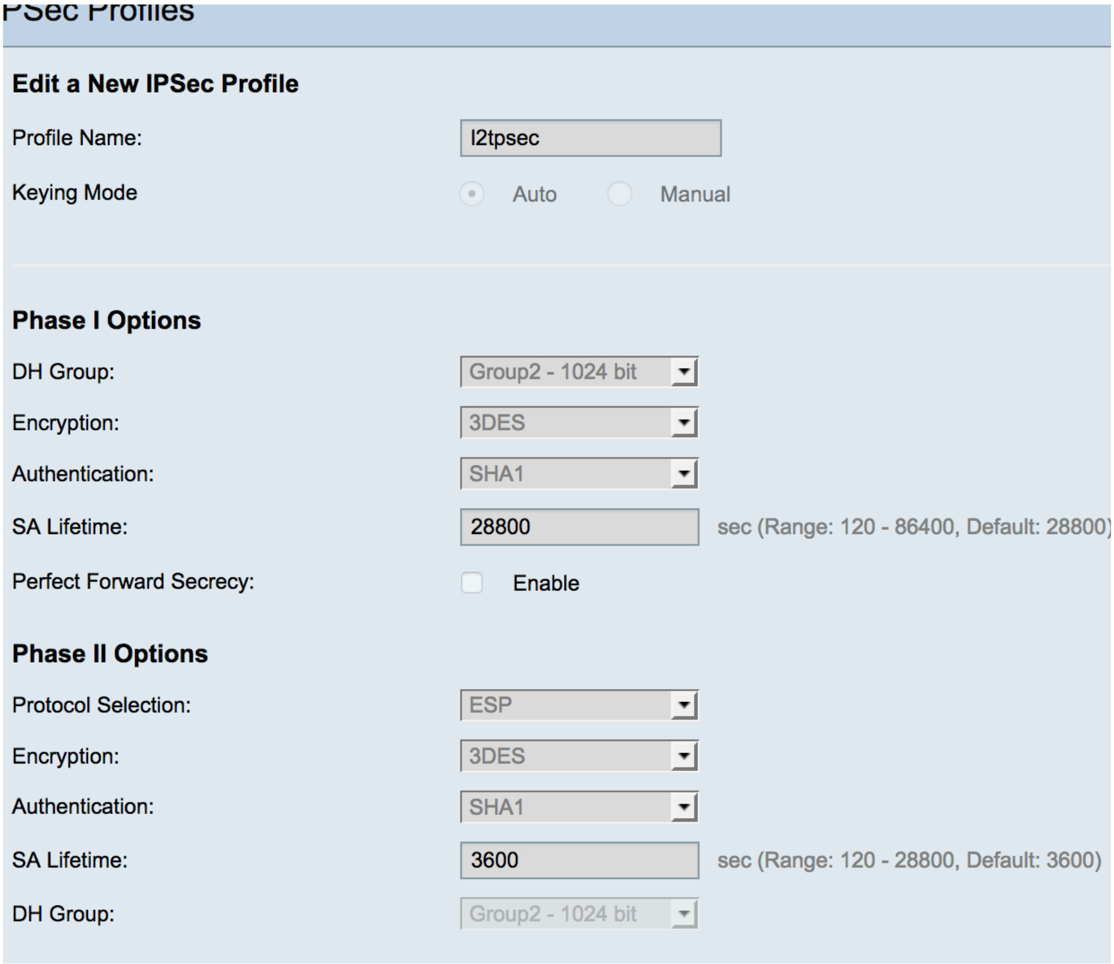
iSL VPN Select a Profile --

'PTP VPN □ Permit

2TP ☑ Permit

Step2:Create new ipsec profile (“l2tpsec”)

The IPSec profile is used to match the IPSec/IKE proposals from the clients. The default profile has PFS enabled which fail to match the Windows client. Below combinations (PFS disabled) can work with Windows10/MACOS/iOS at least.



PSec Profiles

Edit a New IPSec Profile

Profile Name:	l2tpsec	
Keying Mode	● Auto ○ Manual	

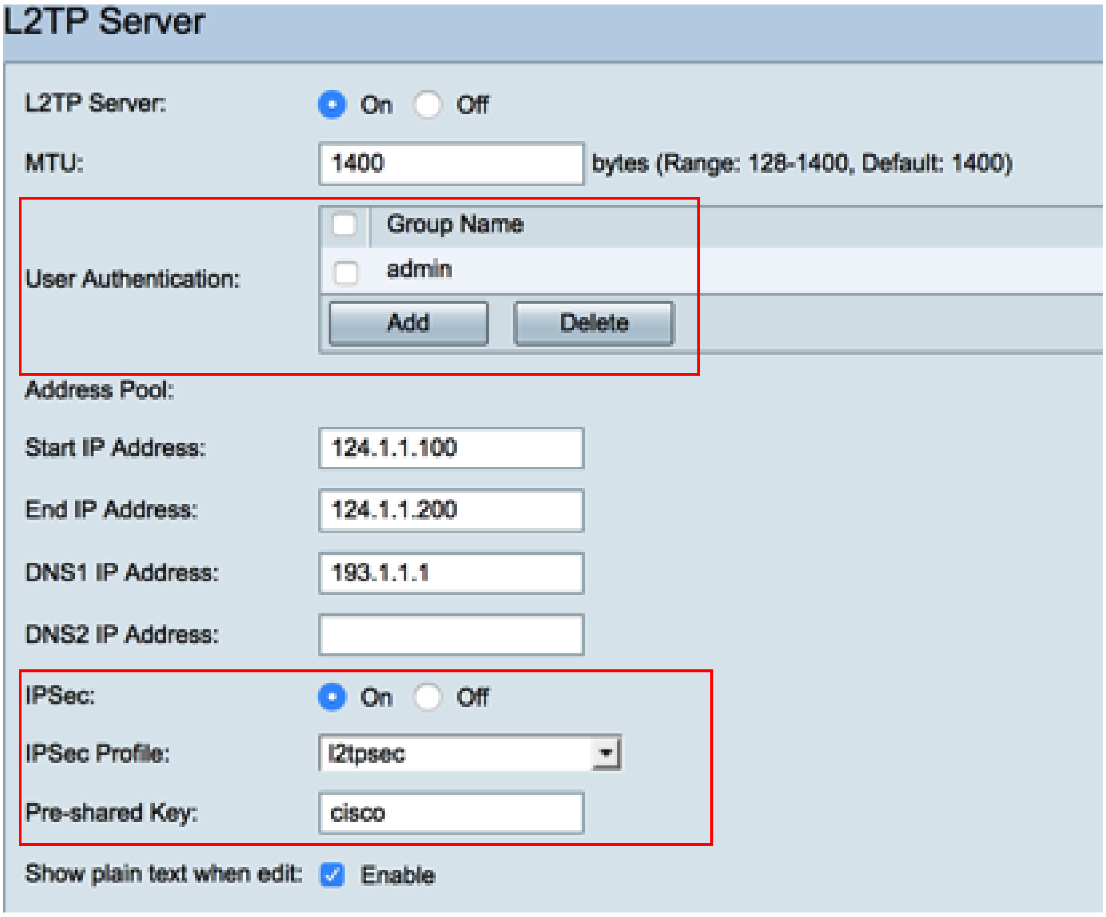
Phase I Options

DH Group:	Group2 - 1024 bit	
Encryption:	3DES	
Authentication:	SHA1	
SA Lifetime:	28800	sec (Range: 120 - 86400, Default: 28800)
Perfect Forward Secrecy:	□ Enable	

Phase II Options

Protocol Selection:	ESP	
Encryption:	3DES	
Authentication:	SHA1	
SA Lifetime:	3600	sec (Range: 120 - 28800, Default: 3600)
DH Group:	Group2 - 1024 bit	

Step3: configure the l2tp server. Choose the groups and IPSec profile configured earlier.



L2TP Server

L2TP Server: ● On ○ Off

MTU: 1400 bytes (Range: 128-1400, Default: 1400)

User Authentication:

□	Group Name
□	admin

Add Delete

Address Pool:

Start IP Address: 124.1.1.100

End IP Address: 124.1.1.200

DNS1 IP Address: 193.1.1.1

DNS2 IP Address:

IPSec: ● On ○ Off

IPSec Profile: l2tpsec

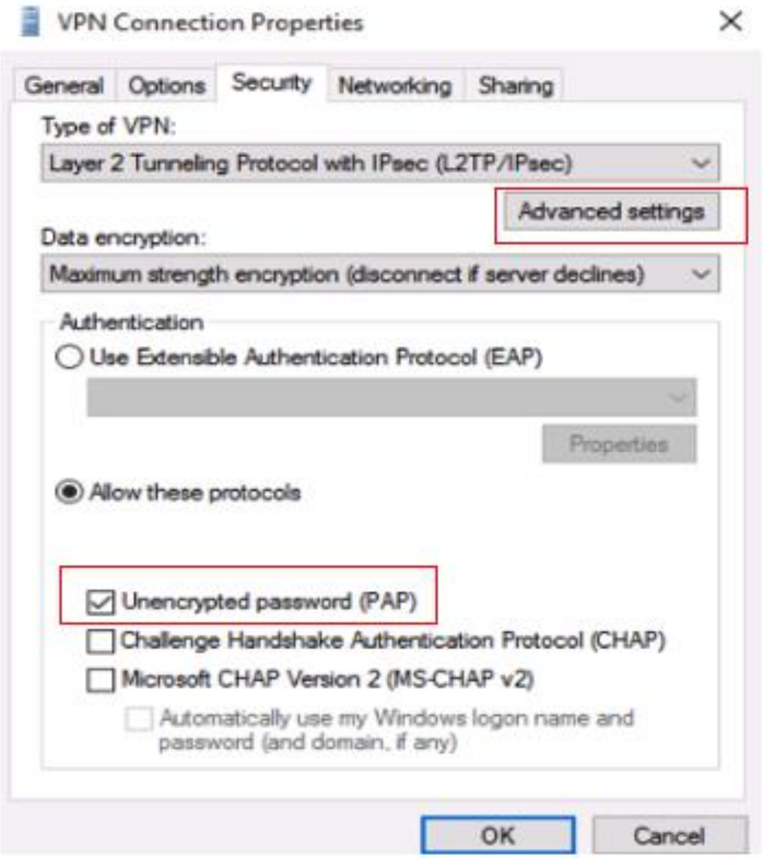
Pre-shared Key: cisco

Show plain text when edit: ☑ Enable

Step4: On Windows 10, create a new VPN connection. Control Panel>Network and Internet>Network and Sharing Center>Setup a new connection or network, create a VPN connection.

Edit the property of this connection, choose L2TP/IPSec, maximum strength encryption or require encryption option. Choose PAP and disable chap/ms-chapv2.

In the “Advanced Settings”, configure the preshared key, “cisco” as configured in step 3.

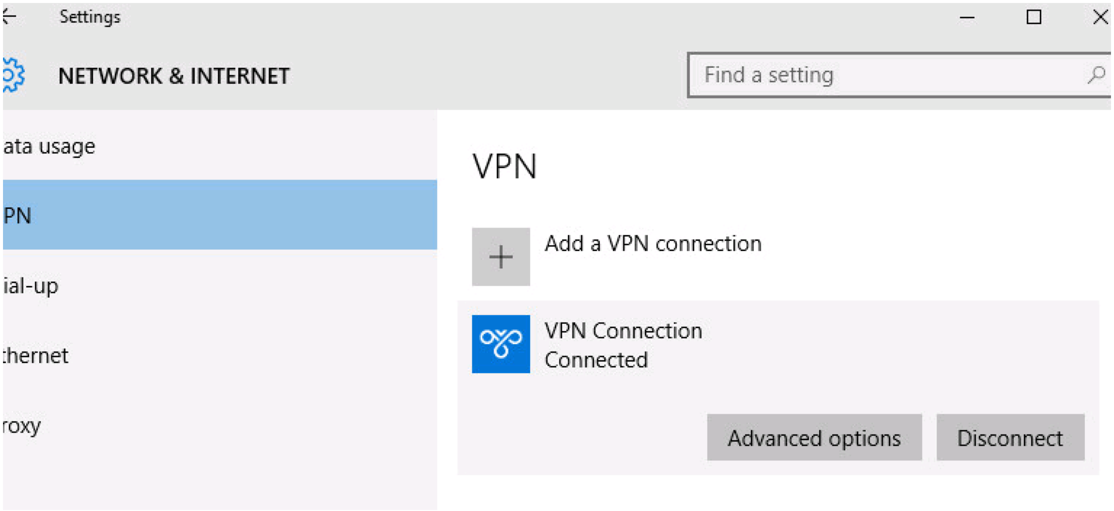


Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Data encryption:
Maximum strength encryption (disconnect if server declines)

Authentication
○ Use Extensible Authentication Protocol (EAP)
● Allow these protocols
☑ Unencrypted password (PAP)
□ Challenge Handshake Authentication Protocol (CHAP)
□ Microsoft CHAP Version 2 (MS-CHAP v2)
□ Automatically use my Windows logon name and password (and domain, if any)

Then the L2TP over ipsec connection can be established.



VPN Connection
Connected

Notes & Tips

1.If use external radius, there are no PAP/CHAP limitations. FreeRadius, Cisco ACS, ISE, etc, can work well with RV340.

2.MACOS doesn't use PAP by default. Below changes are needed to pass pap authentication.

#vim /etc/ppp/options (or create this file if it's not existed)

```
refuse-chap

refuse-mschap

refuse-mschap-v2
```