VPN LAN TO LAN (IPSEC TUNNEL) USING
TP-LINK ARCHER MR200 WITH CISCO
ROUTER

Alexander S
Table of Contents

Introduction .............................................................................................................................................. 2
The Set Up .................................................................................................................................................. 2
Network Diagram ...................................................................................................................................... 3
Configurations .......................................................................................................................................... 3
  Cisco 1841R router .................................................................................................................................. 3
  TP-Link Archer MR200 ............................................................................................................................... 5
Viewing IPSEC VPN status ......................................................................................................................... 6
Introduction

The information with regards to LAN to LAN IPSEC tunnel configuration based on two different networking product on the internet is quite scarce and limited. Almost all 3rd party networking solution is fully compatible with Cisco networking solution particularly related to routing and we could find plenty of documentation about ‘integrating’ 3rd party network equipment with Cisco. TP-Link network product is no exception to this and it is compatible with Cisco network product. But there is an area that I found it quite challenging to overcome (yet I managed to resolve it anyway) when it comes to VPN configuration between Cisco and TP-Link network product. The information on ‘how’ to configure VPN tunnel between these are almost to none. I have not seen any documentation of these so-called Cisco-TP-Link ‘integration’ for IPSEC tunnel on the net. If there is, it is just a small part or a hint which myself not able to grasp.

After quite some time, I finally found a way and write up this document which provides step by step to configure and deploy **LAN to LAN VPN IPSEC tunnel** using Cisco router and TP-Link 4G modem/wireless router.

I hope this document will benefit to those who seek it.

The Set Up

I set up this equipment in my lab environment with access to the local internet service provider (via Metro-E link) and 4G LTE broadband as well. Below is the networking equipment I use in my LAN to LAN VPN IPSEC set up:

- Cisco 1841R router - Cisco IOS software: C1841-ADVIPSERVICESK9-M), Version 12.4(25f)
- TP-Link Archer MR200 – Version 2.0 (Firmware: 1.6.0 0.9.1 v004a.0 Build 181219 Rel.54042n)

Both internet service (Metro-E and 4G LTE broadband) comes with static public IP.
Network Diagram

This document uses this network setup:

![Network Diagram]

**Note:** The IP addressing schemes used in this configuration are not legally routable on the Internet. The external IPs on both sides are fictional. They are RFC 1918 addresses which have been used in a lab environment.

**Configurations**

**Cisco 1841R router**

This configuration presented should be compatible with other Cisco router. When in doubt, kindly consult the latest documentation on Cisco websites. The configuration below shows the essential part of IPSEC VPN tunnel in a Cisco router;

```plaintext
! crypto isakmp policy 100  
enctr 3des  
hash md5  
authentication pre-share  
group 2  
crypto isakmp key VPN-Users address 60.23.45.23  
!  
!  
!--- Pre-share key for both Cisco 1841R router and TP-Link Archer MR200 to establish first stage (Phase 1) of VPN tunnel.
```
--- Create the Phase 2 policy for actual data encryption.

crypto ipsec transform-set RO-VPN esp-3des esp-md5-hmac

--- Create the actual crypto map. Specify
--- the peer IP address, transform
--- set, and an access control list (ACL) for the split tunneling.

crypto map LAN2LAN-VPN 10 ipsec-isakmp
  set peer 60.23.45.23
  set transform-set RO-VPN
  set pfs group2
  match address 100

--- Apply the crypto map on the outside interface.

interface FastEthernet0/0
  description ## Internet ##
  ip address 20.1.1.32 255.255.255.0
  ip virtual-reassembly
duplex auto
  speed auto
  crypto map LAN2LAN-VPN

interface FastEthernet0/1
  description ## Intranet ##
  ip address 172.31.1.254 255.255.255.0
  ip virtual-reassembly
duplex auto
  speed auto

--- Create an ACL for the traffic to
--- be encrypted. In this example,
--- the traffic from 172.31.1.0/24 to 192.168.1.0/24
--- is encrypted. The traffic which does not match the access list
--- is unencrypted for the Internet.

access-list 100 permit ip 172.31.1.0 0.0.0.255 192.168.1.0 0.0.0.255

ip route 0.0.0.0 0.0.0.0 20.1.1.254 1
TP-Link Archer MR200

Configuring IPSec VPN is simple and straightforward. You just need to know and set correct encryption type and method as well as IP address to match with the Cisco router.

To start,

1. Launch and log in to administration web GUI with proper access credential.
2. Under the Advanced section. Navigate the menu until you find IPsec VPN under VPN section.
3. On IPSec Settings page, ensure that Dead Peer Detection is enabled. Click Add (+) to create a new IPSEC connection.
4. Fill up the empty slot as shown below:

<table>
<thead>
<tr>
<th>IPSec Connection Name</th>
<th>Remote-Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote IPSec Gateway (URL)</td>
<td>20.1.1.32</td>
</tr>
<tr>
<td>Tunnel access from local IP addresses</td>
<td>Subnet Address</td>
</tr>
<tr>
<td>IP Address for VPN</td>
<td>192.168.1.0</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Tunnel access from remote IP addresses</td>
<td>Subnet Address</td>
</tr>
<tr>
<td>IP Address for VPN</td>
<td>172.31.1.0</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Key Exchange Method</td>
<td>Auto (IKE)</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>Pre-Shared Key</td>
<td>VPN-Users</td>
</tr>
<tr>
<td>Perfect Forward Secrecy</td>
<td>Enable</td>
</tr>
</tbody>
</table>

Under the Advanced setting page:

<table>
<thead>
<tr>
<th>Phase 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
</tr>
<tr>
<td>Local Identifier Type</td>
</tr>
<tr>
<td>Local Identifier</td>
</tr>
<tr>
<td>Remote Identifier Type</td>
</tr>
<tr>
<td>Remote Identifier</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
</tr>
<tr>
<td>Integrity Algorithm</td>
</tr>
<tr>
<td>Diffie-Hellman Group for Key Exchange</td>
</tr>
<tr>
<td>Key Life Time (Seconds)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Algorithm</td>
</tr>
<tr>
<td>Integrity Algorithm</td>
</tr>
<tr>
<td>Diffie-Hellman Group for Key Exchange</td>
</tr>
<tr>
<td>Key Life Time (Seconds)</td>
</tr>
</tbody>
</table>

5. Once done with these, activate the changes by click OK button. You will be able to view the VPN tunnel status on the page.
Viewing IPSEC VPN status

This section provides information you can use to confirm your configuration is working properly (applicable for Cisco router). Use command `show crypto session` to check the status.

```plaintext
i-Gateway> show crypto session
Crypto session current status
Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 60.23.45.23 port 500
   IKE SA: local 20.1.1.32/500 remote 60.23.45.23 /500 Active
   IPSEC FLOW: permit ip 172.31.1.0/255.255.255.0 192.168.1.0/255.255.255.0
   Active SAs: 2, origin: crypto map

i-Gateway>
```

The session should be UP-ACTIVE. If the session is DOWN or any other status which indicates there is an IPSEC connection issue. You need to make sure both sides’ configuration particularly on encryption method and type should be the same.