

How to use VPN IPsec on TW-EAV510 AC

Note: Please make sure that both LAN side networks are in different subnet.

Setup VPN IPsec Function

Go to **WAN -> VPN -> IPsec**, IPsec don't need enable/ disable, user can setup directly. Like as below pic.

IPsec Configuration

This page is used to configure the parameters for IPsec mode VPN.

Remote:

IPsec gateway address	<input type="text" value="0.0.0.0"/>
LAN IP address	<input type="text" value="0.0.0.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>

Local:

WAN IP address	<input type="text" value="0.0.0.0"/>
LAN IP address	<input type="text" value="0.0.0.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>

Security Option:

Encapsulation Type	<input type="text" value="ESP"/>
Pre-Shared Key	<input type="text"/>
Advanced Options	<input type="checkbox"/>

Key Life Time							
Enable	State	Type	IPsec gateway address	Remote Network	WAN IP address	Local Network	Mode
<input type="button" value="Delete Selected"/>							
<input type="button" value="Enable"/>							
<input type="button" value="Disable"/>							

Remote:

IPsec Gateway address: Enter the remote side WAN IP or domain.

LAN IP address: Enter the remote router LAN IP.

Subnet Mask: Enter the remote network's netmask.

Local:

WAN IP address: Enter the local router WAN IP, not necessary input, system will automatically enter.

LAN IP address: Enter the local router LAN IP, not necessary input, system will automatically enter.

Subnet Mask: Enter the local network's netmask.

Security Option:

Encapsulation Type: Define the encapsulation type for IPSec

Pre-Shared Key: The password will be used for both side authentication.

Advances Options: Make it checked to shows more settings, see below pic.

Advanced Options

IKE Phase 1:

Mode

IKE Algorithm

Encryption Algorithm

Integrity Algorithm

Select Diffie-Hellman Group

IKE Phase 2:

Security Algorithm

Encryption Algorithm

Integrity Algorithm

Select Diffie-Hellman Group

IKE Phase 1:

Mode: Select the mode for IPSec Phase 1.

Encryption Algorithm: Define the encryption algorithm for Phase 1.

Integrity Algorithm: Define the integrity algorithm for Phase 1.

Select Diffie-Hellman Group for Key Exchange: Define the Diffie_Hellman for Phase 1.

IKE Phase 2:

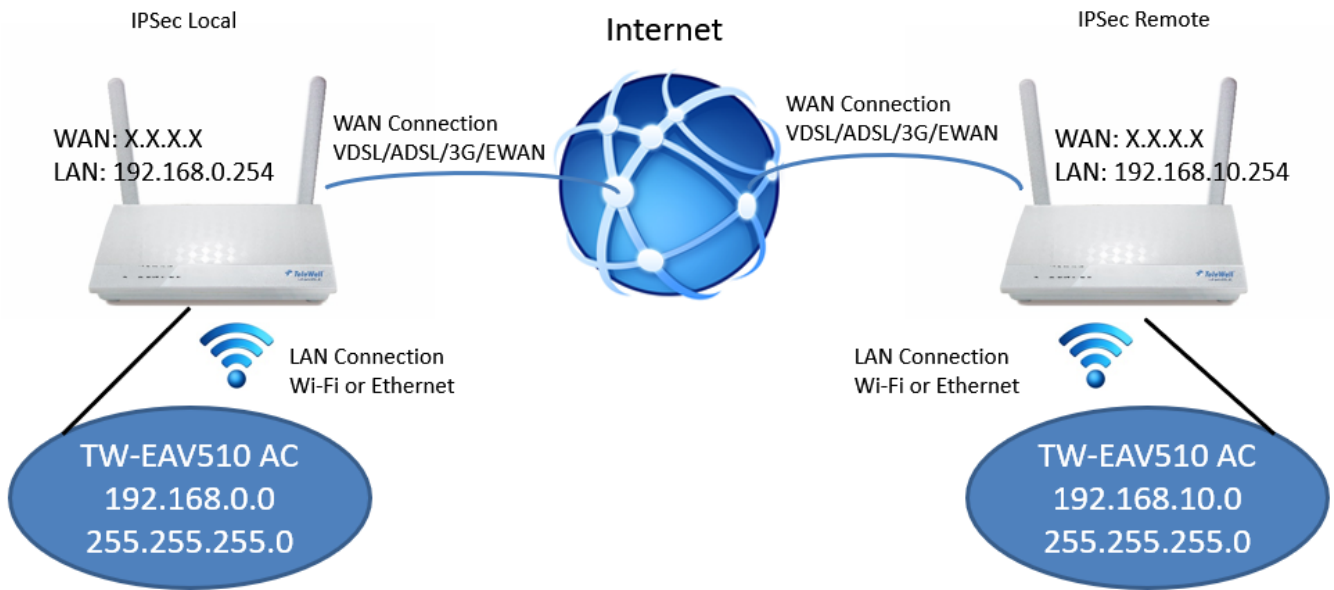
Encryption Algorithm: Define the encryption algorithm for IPSec Phase 2.

Integrity Algorithm: Define the integrity algorithm for Phase 2.

Select Diffie-Hellman Group for Key Exchange: Define the Diffie_Hellman for Phase 2.

Example 1

Both TW-EAV510 AC are enable IPsec function. IPSec is point-to-point, no server and client distinguish.



Remote Side

TW-EAV510 AC

1. Go to **WAN** -> **VPN** -> **IPSec**, in **Remote** part fill in other side WAN IP or domain, router LAN IP, for **Local** part, isn't necessary fill in, because system will automatically enter, input Pre-Shared Key for authenticate, like as below picture.

This page is used to configure the parameters for IPsec mode VPN.

Remote:

IPSec gateway address	<input type="text" value="36.229.14.220"/>
LAN IP address	<input type="text" value="192.168.0.254"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>

Local:

WAN IP address	<input type="text" value="0.0.0.0"/>
LAN IP address	<input type="text" value="0.0.0.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>

Security Option:

Encapsulation Type	<input type="text" value="ESP"/>
Pre-Shared Key	<input type="text" value="psk12345678"/>
Advanced Options	<input type="checkbox"/>

Click **Add/Save** button to save changes.

2. After Add the new config, **Key Life Time** would add one connection, user can disable/enable or delete selected.

Key Life Time								
	Enable	State	Type	IPSec gateway address	Remote Network	WAN IP address	Local Network	Mode
<input type="checkbox"/>	Enable	Established	AUTO	36.229.14.220	192.168.0.254	0.0.0.0	192.168.10.254	ESP

Local Side

1. Go to **WAN -> VPN -> IPSec**, input other side router WAN IP like as below picture.

This page is used to configure the parameters for IPsec mode VPN.

Remote:

IPSec gateway address
 LAN IP address
 Subnet Mask

Local:

WAN IP address
 LAN IP address
 Subnet Mask

Security Option:

Encapsulation Type
 Pre-Shared Key
 Advanced Options

Click **Add/Save** button to save changes.

2. After Add the new config, **Key Life Time** would add one connection, user can disable/enable or delete selected.

Key Life Time								
	Enable	State	Type	IPSec gateway address	Remote Network	WAN IP address	Local Network	Mode
<input type="checkbox"/>	Enable	Established	AUTO	36.225.80.226	192.168.10.254	0.0.0.0	192.168.0.254	ESP

3. After both side setup ready, use PC launch CMD, try to ping other side PC, first time should be time out then would ping successfully. Now you can access to remote network.

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:
Request timed out.
Reply from 192.168.10.100: bytes=32 time=16ms TTL=126
Reply from 192.168.10.100: bytes=32 time=11ms TTL=126
Reply from 192.168.10.100: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 16ms, Average = 13ms

C:\WINDOWS\system32>ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :

Ethernet adapter 乙太網路:

    Connection-specific DNS Suffix . . . . . : telewell.oy
    Link-local IPv6 Address . . . . . : fe80::f109:45a5:c12f:8ef6%20
    IPv4 Address. . . . . : 192.168.0.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.254
```