IPSec_Pre shared key and Xauth with CISCO router

1. Introduction

1.1 Overview

This document contains information regarding the configuration and use of IPSec_Pre-shared key and Xauth with CISCO router.

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

1.2 Compatibility

This application note applies to:

Models Shown: 641M series.

Firmware Version: V1.0.0 (903.0) or newer

Other Compatible Models: None

1.3 Version

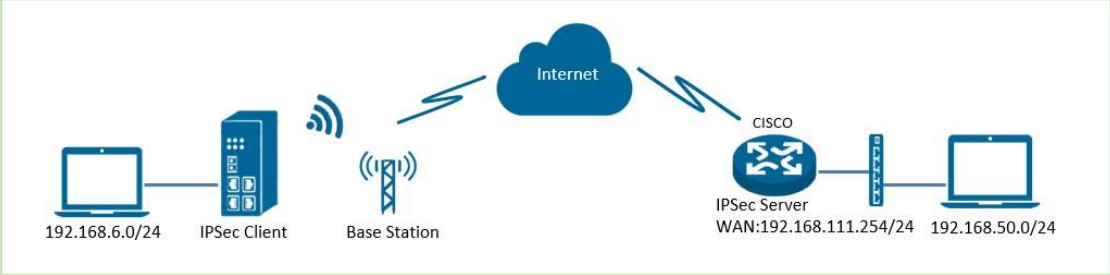
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2018/08/03	V1.0.0	V1.0.0 (903.0)	First released

1.4 Corrections

Appreciate for corrections or rectifications to this application note, and if any request for new application notes please email to: support@elpro.com.au

2. Topology



1. 641M runs as IPSec Client with any kind of IP, which can ping IPSec server IP successfully.
2. CISCO router runs as IPSec Server with a static public IP.
3. IPSec tunnel is established between 641M and cisco router.

3. Configuration

3.1 Server Configuration

1. Login to CISCO router and setting like below:

==========

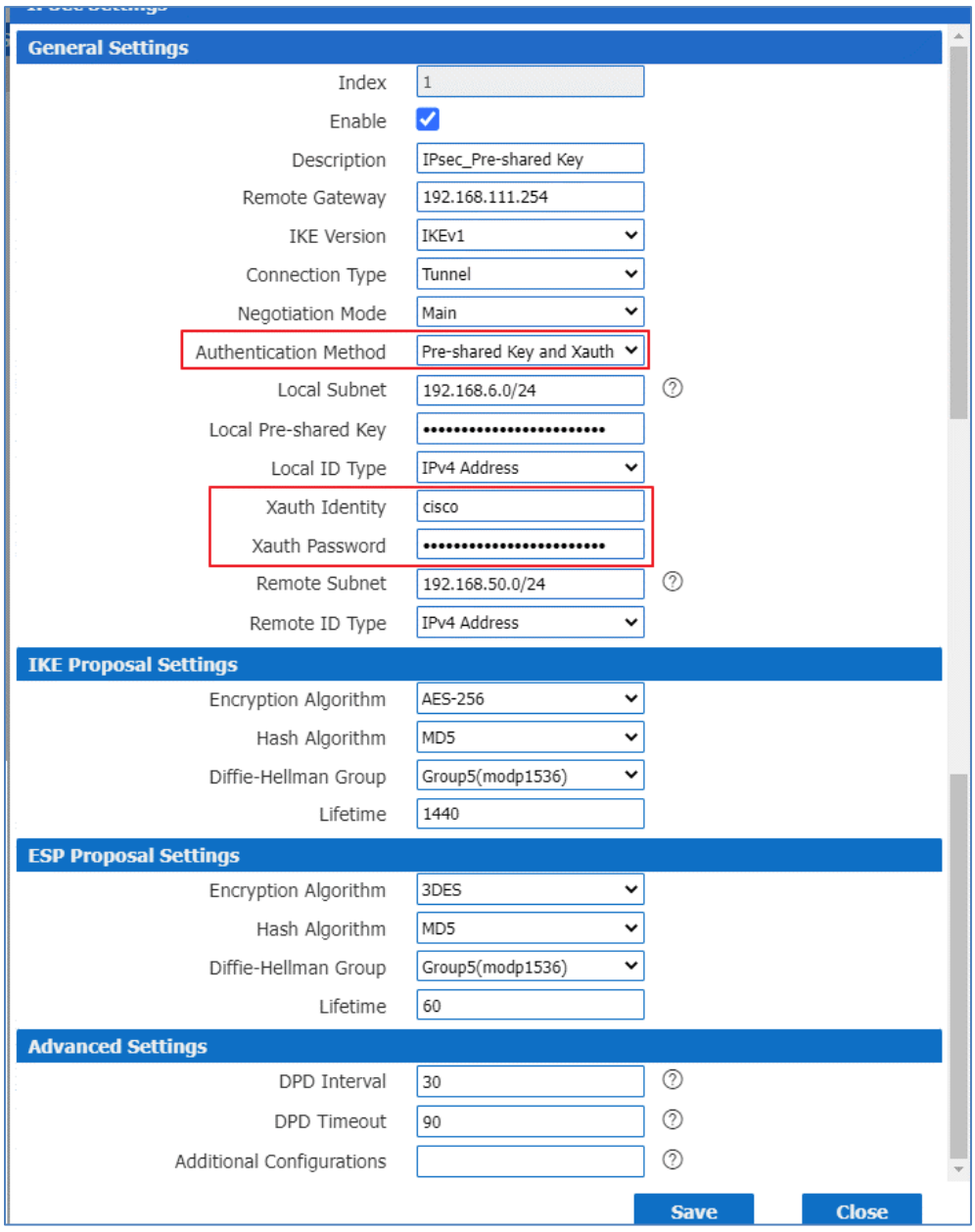
```
cisco2811#show running
config
version 12.4
hostname cisco2811
!
enable secret 5 $1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.
new-model
authentication login LOGIN local
!
session
id common
dot11 syslog
ip source route
!
ip cef
ip domain name cisco.com
ip name
server 192.168.111.1
ip address pool local
no ipv6 cef
!
username cisco password 0 cisco
archive
log config
hidekeys
!
crypto isakmp policy 10
encr aes 256
hash md5
authentication pre share
group 5
crypto isakmp key 6 cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set 641M esp 3des esp md5 hmac
!
```

```
crypto dynamic-map DYN 10
set transform set 641M
set pfs group5
match address 101
reverse-route
!
crypto map MAP client authentication list LOGIN
crypto map MAP 10 ipsec--isakmp dynamic DYN
!
track 1 interface FastEthernet0/0 line
protocol
interface Loopback0
ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
ip address 192.168.111.254 255.255.255.0
ip nat outside
ip nat enable
ip virtual reassembly
duplex full
speed auto
no mop enabled
crypto map MAP
!
interface FastEthernet0/1
ip address 192.168.5.1 255.255.255.0
ip nat inside
ip nat enable
ip virtual reassembly
duplex auto
speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface FastEthernet0/0 overload
!
ip access-list extended VPN
permit ip 192.168.50.0 0.0.0.255 192.1 68.6.0 0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
```

!!
line con 0
line vty 5 15
exec timeout 5 2
end
==========

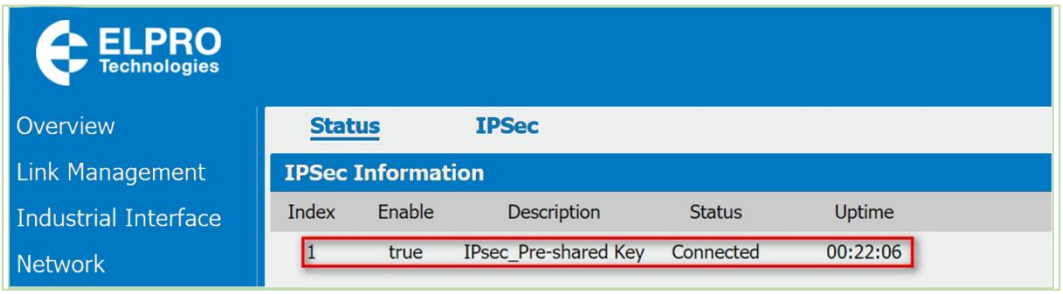
3.2 Client Configuration

1. Go to **VPN>IPSec>IPSec>General Settings**, click the Edit Button and configure IPSec VPN as per below picture. Click Save.



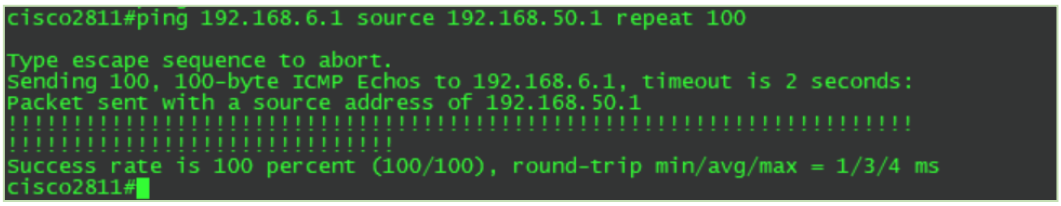
2. Click Save>Apply.

3. IPSec had been connected successfully. Go to **VPN>IPSec>Status** to check the connection status.

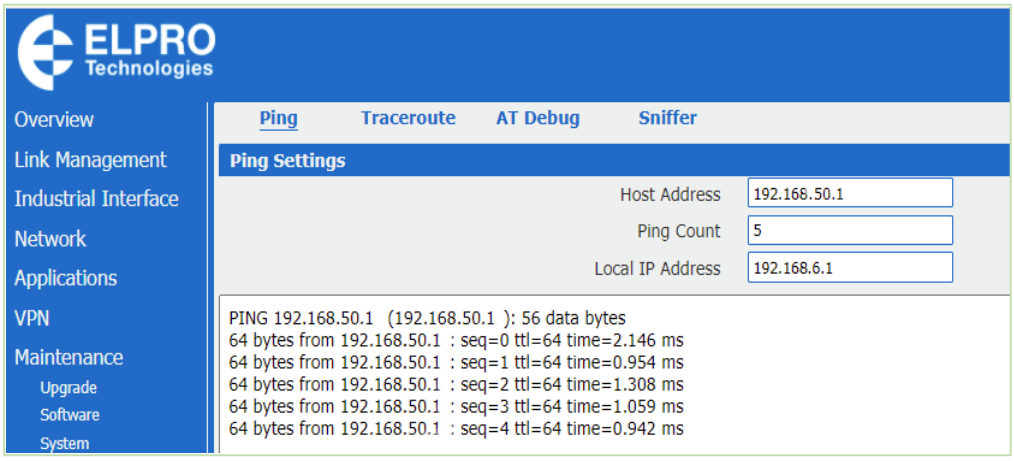


4. Testing

1. Ping from CISCO router to 641M, LAN to LAN communication is working correctly.



2. Ping from 641M to CISCO router, LAN to LAN communication is working correctly.



3. Test successfully.