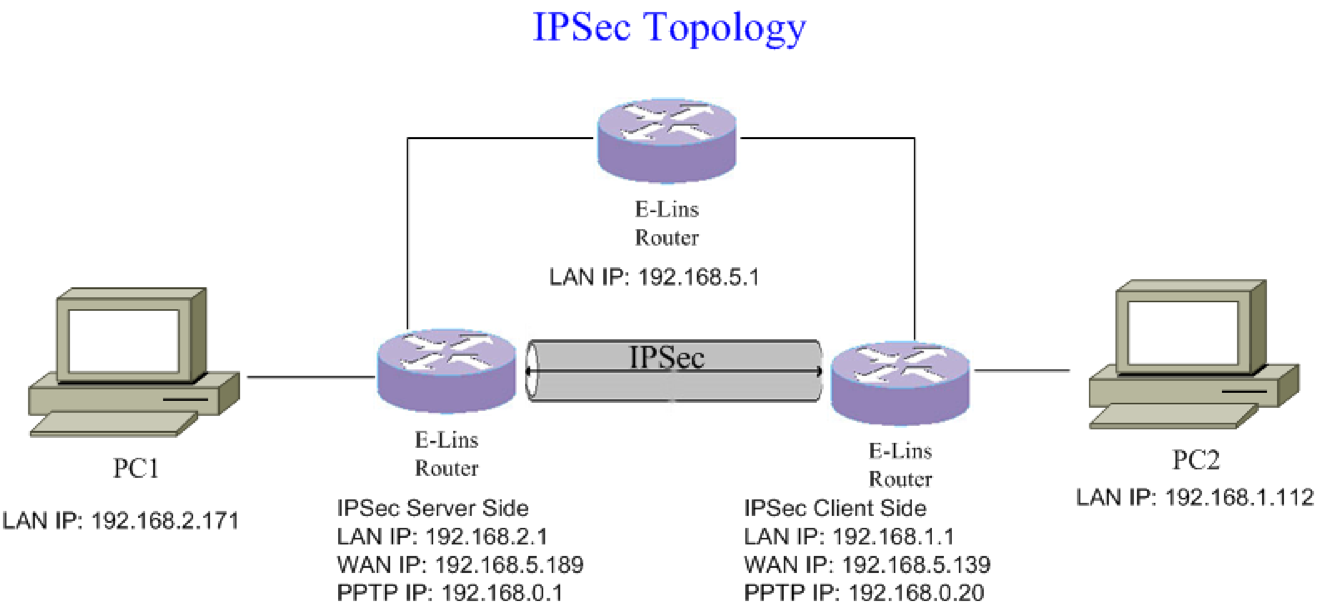
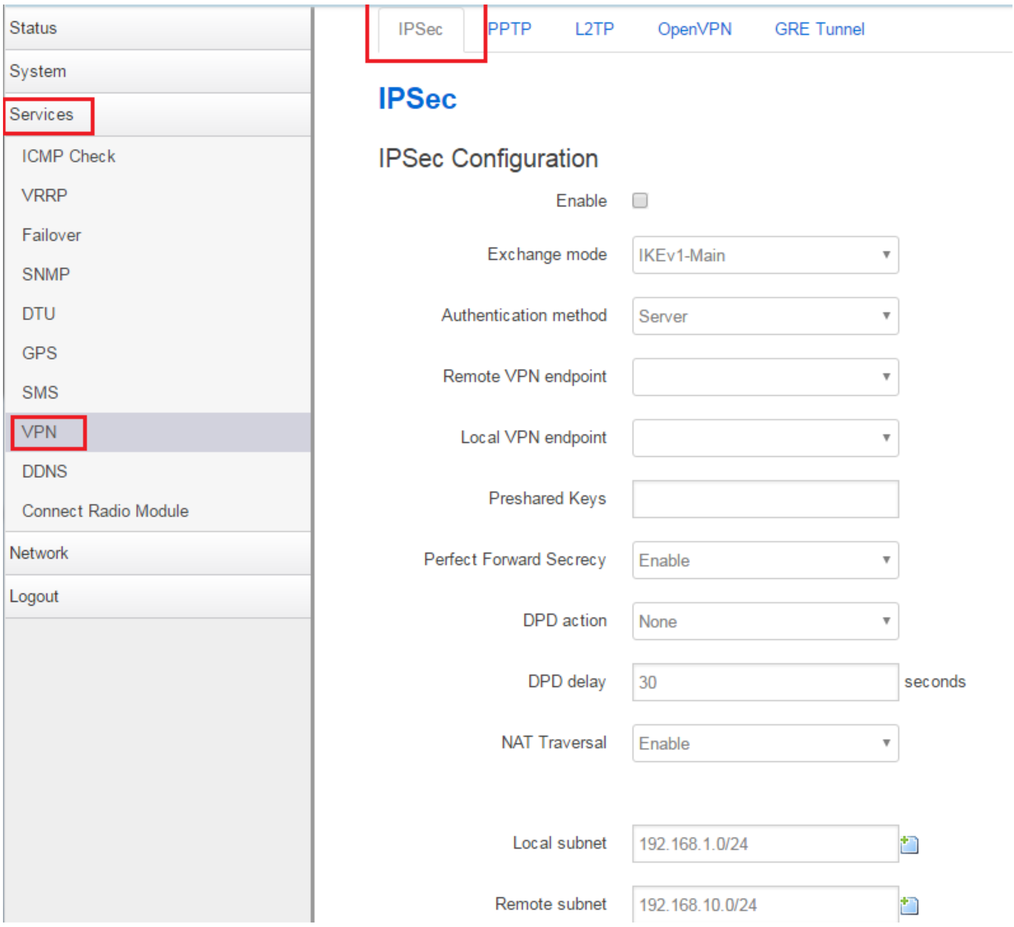
VPN Example - IPSec



IPSec Server configuration

1. Open web management page. Click “Services” → “VPN” at the left navigation bar.



IPSec

IPSec Configuration

Enable □

Exchange mode: IKEv1-Main

Authentication method: Server

Remote VPN endpoint:

Local VPN endpoint:

Preshared Keys:

Perfect Forward Secrecy: Enable

DPD action: None

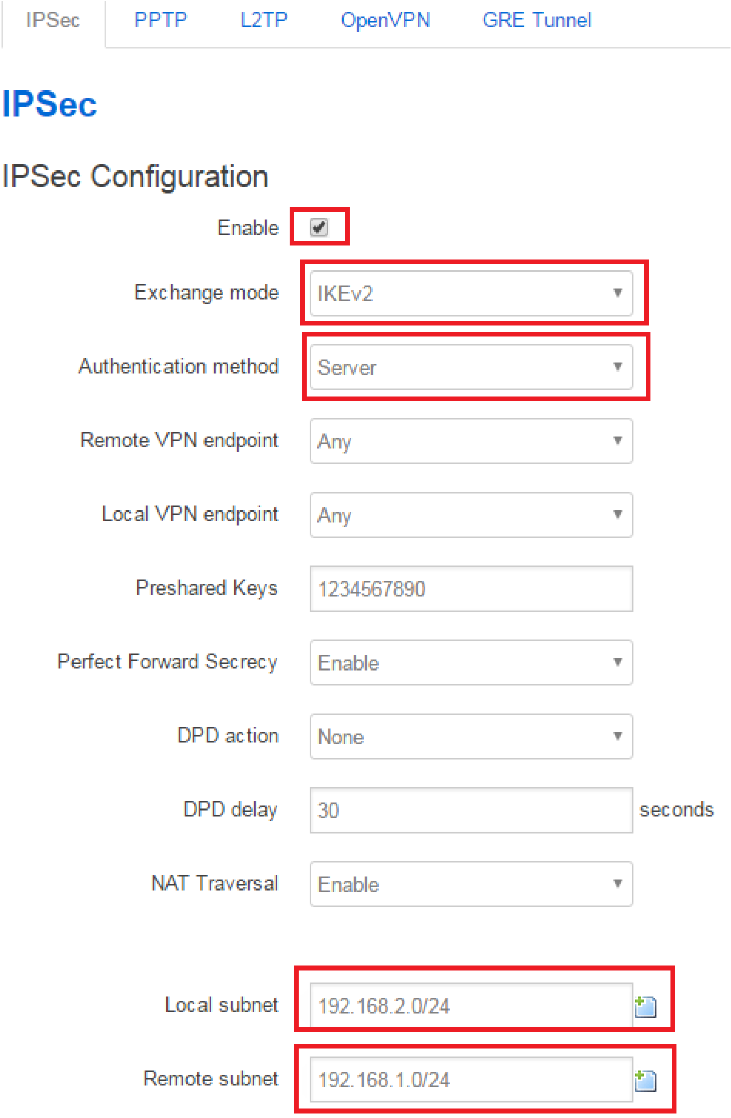
DPD delay: 30 seconds

NAT Traversal: Enable

Local subnet: 192.168.1.0/24

Remote subnet: 192.168.10.0/24

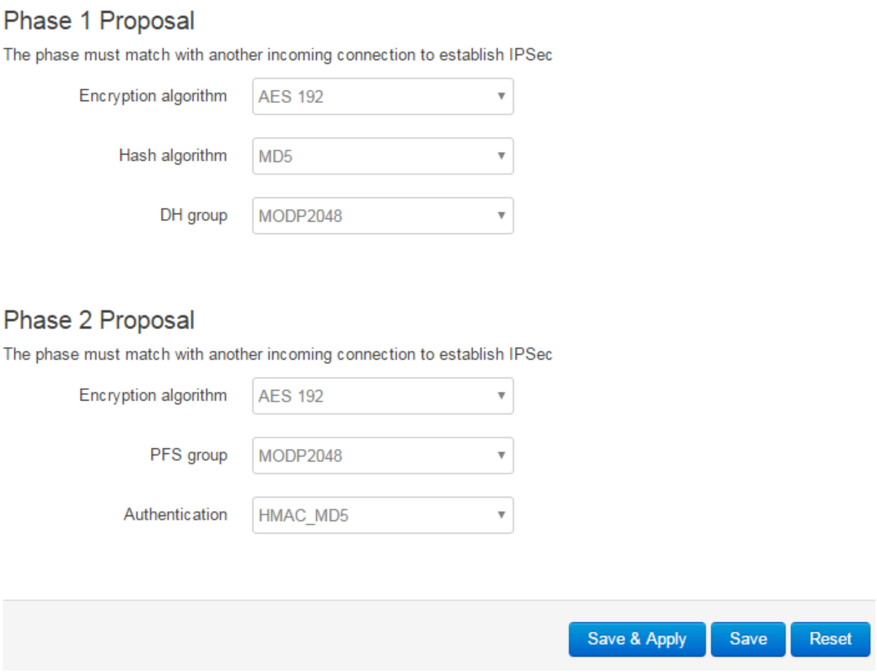
2. Check “Enable”, select IKEv2 as Exchange mode, set Authentication method to Server. Set local LAN subnet and remote LAN subnet accordingly.



IPSec

IPSec Configuration

Enable	☑
Exchange mode	IKEv2
Authentication method	Server
Remote VPN endpoint	Any
Local VPN endpoint	Any
Preshared Keys	1234567890
Perfect Forward Secrecy	Enable
DPD action	None
DPD delay	30 seconds
NAT Traversal	Enable
Local subnet	192.168.2.0/24
Remote subnet	192.168.1.0/24



Phase 1 Proposal

The phase must match with another incoming connection to establish IPSec

Encryption algorithm: AES 192

Hash algorithm: MD5

DH group: MODP2048

Phase 2 Proposal

The phase must match with another incoming connection to establish IPSec

Encryption algorithm: AES 192

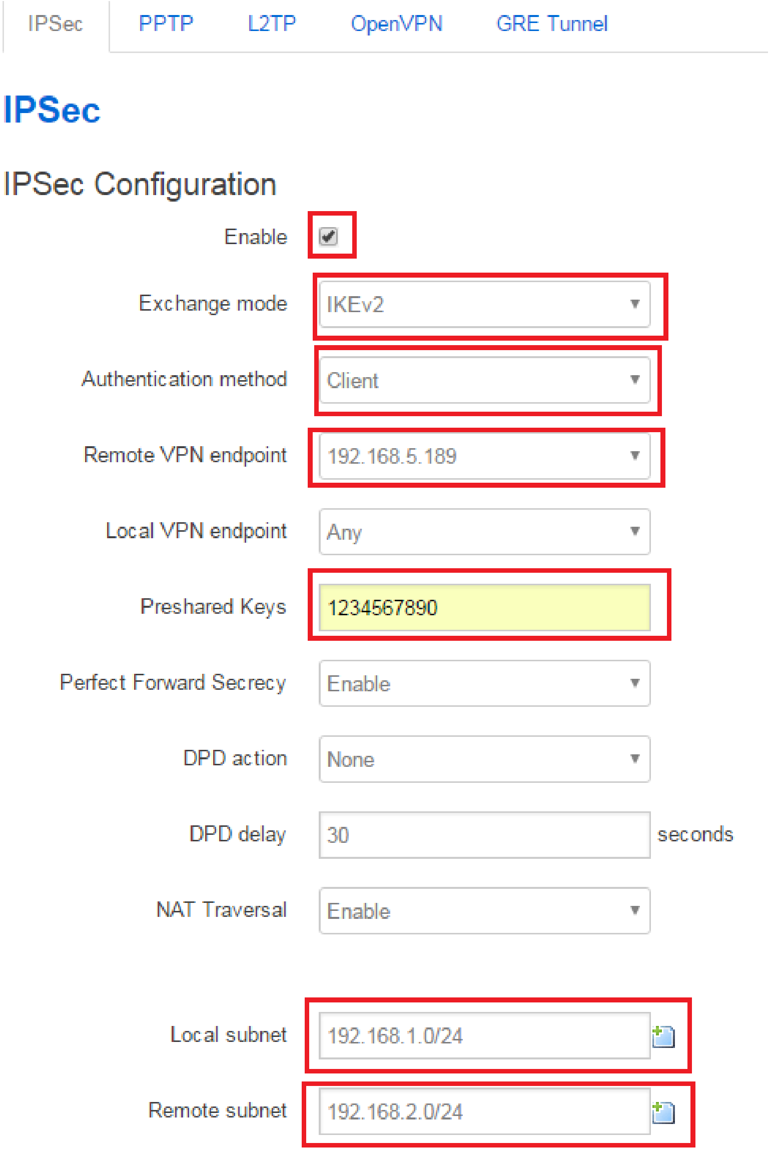
PFS group: MODP2048

Authentication: HMAC_MD5

3. After all settings is done, click button “Save & Apply”.

IPSec Client configuration

1. Open web management page. Click “Services” → “VPN” at the left navigation bar.
2. Check “Enable”, select IKEv2 as Exchange mode, set Authentication method to “Client”. Set local LAN subnet and remote LAN subnet accordingly. Preshared Keys shall be same as server side. Remote VPN endpoint is server WAN IP address.

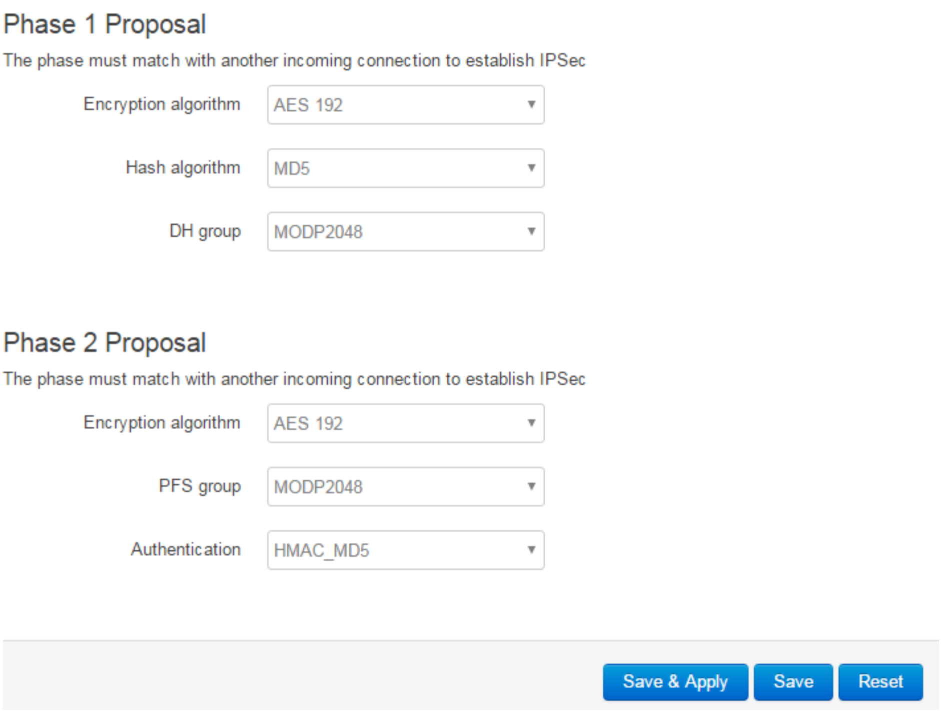


IPSec

IPSec Configuration

Enable	☑
Exchange mode	IKEv2
Authentication method	Client
Remote VPN endpoint	192.168.5.189
Local VPN endpoint	Any
Preshared Keys	1234567890
Perfect Forward Secrecy	Enable
DPD action	None
DPD delay	30 seconds
NAT Traversal	Enable
Local subnet	192.168.1.0/24
Remote subnet	192.168.2.0/24

3. Set Phase 1 and Phase 2, it must match with server side.



Phase 1 Proposal

The phase must match with another incoming connection to establish IPSec

Encryption algorithm: AES 192

Hash algorithm: MD5

DH group: MODP2048

Phase 2 Proposal

The phase must match with another incoming connection to establish IPSec

Encryption algorithm: AES 192

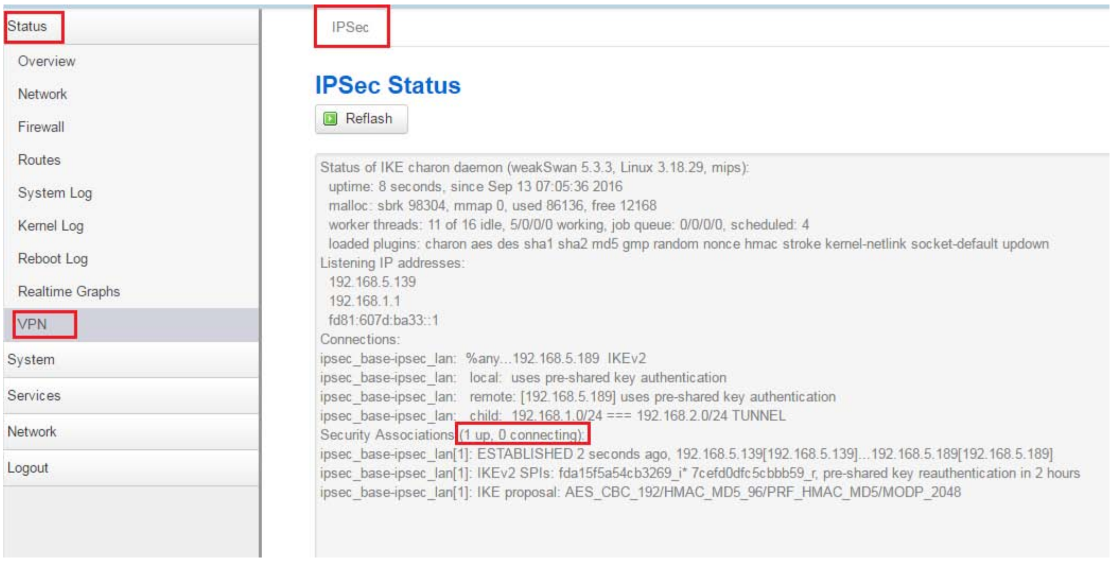
PFS group: MODP2048

Authentication: HMAC_MD5

4. After all settings is done, click button “Save & Apply”.

IPsec Status

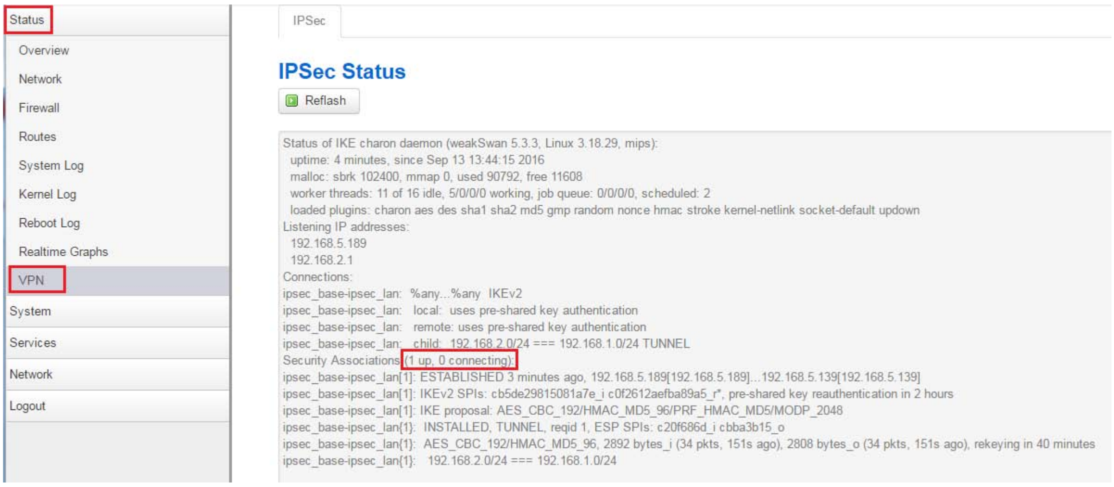
1. Check IPSec status at client side. Click “Status” → “VPN” at left navigation bar, there is 1 connection is up.



IPSec Status

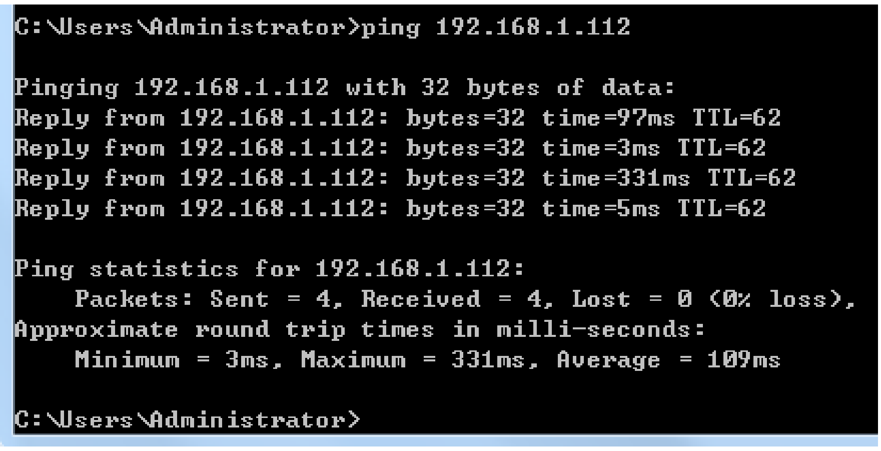
```
Status of IKE charon daemon (weakSwan 5.3.3, Linux 3.18.29, mips):
  uptime: 8 seconds, since Sep 13 07:05:36 2016
  malloc: sbrk 98304, mmap 0, used 86136, free 12168
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon aes des sha1 sha2 md5 gmp random nonce hmac stroke kernel-netlink socket-default updown
Listening IP addresses:
  192.168.5.139
  192.168.1.1
  fd81:607d:ba33::1
Connections:
ipsec_base-ipsec_lan:  %any...192.168.5.189  IKEv2
ipsec_base-ipsec_lan:   local:  uses pre-shared key authentication
ipsec_base-ipsec_lan:   remote: [192.168.5.189] uses pre-shared key authentication
ipsec_base-ipsec_lan:   child:  192.168.1.0/24 === 192.168.2.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
ipsec_base-ipsec_lan[1]: ESTABLISHED 2 seconds ago, 192.168.5.139[192.168.5.139]...192.168.5.189[192.168.5.189]
ipsec_base-ipsec_lan[1]: IKEv2 SPIs: fda15f5a54cb3269_i* 7cefd0dfc5cbbb59_r, pre-shared key reauthentication in 2 hours
ipsec_base-ipsec_lan[1]: IKE proposal: AES_CBC_192/HMAC_MD5_96/PRF_HMAC_MD5/MODP_2048
```

2. Check IPSec status at server side. Click “Status” → “VPN” at left navigation bar, there is 1 connection is up.



```
Status of IKE charon daemon (weakSwan 5.3.3, Linux 3.18.29, mips):
  uptime: 4 minutes, since Sep 13 13:44:15 2016
  malloc: sbrk 102400, mmap 0, used 90792, free 11608
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
  loaded plugins: charon aes des sha1 sha2 md5 gmp random nonce hmac stroke kernel-netlink socket-default updown
Listening IP addresses:
  192.168.5.189
  192.168.2.1
Connections:
ipsec_base-ipsec_lan:  %any...%any  IKEv2
ipsec_base-ipsec_lan:   local:  uses pre-shared key authentication
ipsec_base-ipsec_lan:   remote: uses pre-shared key authentication
ipsec_base-ipsec_lan:   child:  192.168.2.0/24 === 192.168.1.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
ipsec_base-ipsec_lan[1]: ESTABLISHED 3 minutes ago, 192.168.5.189[192.168.5.189]...192.168.5.139[192.168.5.139]
ipsec_base-ipsec_lan[1]: IKEv2 SPIs: cb5de29815081a7e_i c0f2612aefba89a5_r*, pre-shared key reauthentication in 2 hours
ipsec_base-ipsec_lan[1]: IKE proposal: AES_CBC_192/HMAC_MD5_96/PRF_HMAC_MD5/MODP_2048
ipsec_base-ipsec_lan{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c20f686d_i cbba3b15_o
ipsec_base-ipsec_lan{1}:  AES_CBC_192/HMAC_MD5_96, 2892 bytes_i (34 pkts, 151s ago), 2808 bytes_o (34 pkts, 151s ago), rekeying in 40 minutes
ipsec_base-ipsec_lan{1}:   192.168.2.0/24 === 192.168.1.0/24
```

3. Ping PC 192.168.1.112 from PC 192.168.2.171



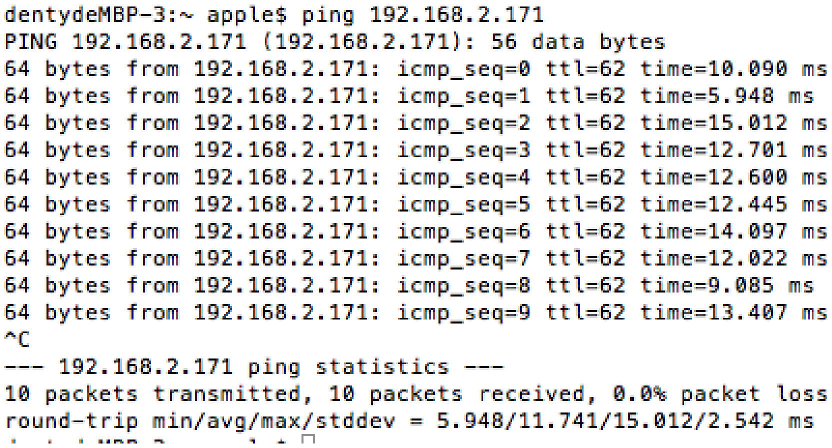
```
C:\Users\Administrator>ping 192.168.1.112

Pinging 192.168.1.112 with 32 bytes of data:
Reply from 192.168.1.112: bytes=32 time=97ms TTL=62
Reply from 192.168.1.112: bytes=32 time=3ms TTL=62
Reply from 192.168.1.112: bytes=32 time=331ms TTL=62
Reply from 192.168.1.112: bytes=32 time=5ms TTL=62

Ping statistics for 192.168.1.112:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 331ms, Average = 109ms

C:\Users\Administrator>
```

4. Ping PC 192.168.2.171 from PC 192.168.1.112



```
dentydeMBP-3:~ apple$ ping 192.168.2.171
PING 192.168.2.171 (192.168.2.171): 56 data bytes
64 bytes from 192.168.2.171: icmp_seq=0 ttl=62 time=10.090 ms
64 bytes from 192.168.2.171: icmp_seq=1 ttl=62 time=5.948 ms
64 bytes from 192.168.2.171: icmp_seq=2 ttl=62 time=15.012 ms
64 bytes from 192.168.2.171: icmp_seq=3 ttl=62 time=12.701 ms
64 bytes from 192.168.2.171: icmp_seq=4 ttl=62 time=12.600 ms
64 bytes from 192.168.2.171: icmp_seq=5 ttl=62 time=12.445 ms
64 bytes from 192.168.2.171: icmp_seq=6 ttl=62 time=14.097 ms
64 bytes from 192.168.2.171: icmp_seq=7 ttl=62 time=12.022 ms
64 bytes from 192.168.2.171: icmp_seq=8 ttl=62 time=9.085 ms
64 bytes from 192.168.2.171: icmp_seq=9 ttl=62 time=13.407 ms
^C
--- 192.168.2.171 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 5.948/11.741/15.012/2.542 ms
```