```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ipsec.conf
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ipsec.secrets
```

```
config setup
    charondebug="ike 2, knl 2, cfg 2"

conn right-to-left
    auto=add
    keyexchange=ikev2
    type=tunnel

    left=192.168.217.130
    leftid=192.168.217.130
    leftsubnet=192.168.217.130/32

    right=192.168.217.129
    rightid=192.168.217.129
    rightsubnet=192.168.217.129/32

    ike=aes256-sha256-modp2048
    esp=aes256-sha256
    authby=psk
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ipsec start
Starting strongSwan 6.0.3 IPsec [starter]...

┌──(kali㉿kali)-[~]
└─$ sudo ipsec up right-to-left
initiating IKE_SA right-to-left[1] to 192.168.217.129
generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
sending packet: from 192.168.217.130[500] to 192.168.217.129[500] (1208 bytes)
retransmit 1 of request with message ID 0
sending packet: from 192.168.217.130[500] to 192.168.217.129[500] (1208 bytes)
retransmit 2 of request with message ID 0
sending packet: from 192.168.217.130[500] to 192.168.217.129[500] (1208 bytes)
retransmit 3 of request with message ID 0
sending packet: from 192.168.217.130[500] to 192.168.217.129[500] (1208 bytes)
retransmit 4 of request with message ID 0
sending packet: from 192.168.217.130[500] to 192.168.217.129[500] (1208 bytes)
retransmit 5 of request with message ID 0
sending packet: from 192.168.217.130[500] to 192.168.217.129[500] (1208 bytes)
^Z
zsh: suspended  sudo ipsec up right-to-left
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 6.0.3, Linux 6.12.25-amd64, x86_64):
  uptime: 3 minutes, since Nov 25 00:32:52 2025
  malloc: sbrk 2867200, mmap 270336, used 979376, free 1887824
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon aesni random nonce x509 revocation constraints pubkey pkcs1 pkcs7 dnskey sshkey pem openssl pkcs8 agent gcm drbg attr k
ernel-netlink resolve socket-default connmark stroke updown eap-mschapv2 xauth-generic counters
Listening IP addresses:
  192.168.217.130
Connections:
right-to-left:  192.168.217.130...192.168.217.129  IKEv2
right-to-left:   local:  [192.168.217.130] uses pre-shared key authentication
right-to-left:   remote: [192.168.217.129] uses pre-shared key authentication
right-to-left:   child:  192.168.217.130/32 === 192.168.217.129/32 TUNNEL
Security Associations (1 up, 0 connecting):
right-to-left[1]: ESTABLISHED 51 seconds ago, 192.168.217.130[192.168.217.130]...192.168.217.129[192.168.217.129]
right-to-left[1]: IKEv2 SPIs: 82b3ff6dd6f204fd_i* 6d1bd32f6fe8315b_r, pre-shared key reauthentication in 2 hours
right-to-left[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
right-to-left{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c32476fe_i c72b49eb_o
right-to-left{2}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 43 minutes
right-to-left{2}:   192.168.217.130/32 === 192.168.217.129/32
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.217.129
PING 192.168.217.129 (192.168.217.129) 56(84) bytes of data.
64 bytes from 192.168.217.129: icmp_seq=1 ttl=64 time=0.733 ms
64 bytes from 192.168.217.129: icmp_seq=2 ttl=64 time=0.919 ms
64 bytes from 192.168.217.129: icmp_seq=3 ttl=64 time=0.845 ms
64 bytes from 192.168.217.129: icmp_seq=4 ttl=64 time=1.16 ms
64 bytes from 192.168.217.129: icmp_seq=5 ttl=64 time=0.499 ms
64 bytes from 192.168.217.129: icmp_seq=6 ttl=64 time=0.650 ms
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ipsec.conf
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ipsec.secrets
```

```
config setup
    charondebug="ike 2, knl 2, cfg 2"

conn left-to-right
    auto=add
    keyexchange=ikev2
    type=tunnel

    left=192.168.217.129
    leftid=192.168.217.129
    leftsubnet=192.168.217.129/32

    right=192.168.217.130
    rightid=192.168.217.130
    rightsubnet=192.168.217.130/32

    ike=aes256-sha256-modp2048
    esp=aes256-sha256
    authby=psk
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 6.0.3, Linux 6.12.25-amd64, x86_64):
  uptime: 118 seconds, since Nov 25 00:34:42 2025
  malloc: sbrk 2867200, mmap 270336, used 984848, free 1882352
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon aesni random nonce x509 revocation constraints pubkey pkcs1 pkcs7 dnskey sshkey pem openssl pkcs8 agent gcm drbg attr k
ernel-netlink resolve socket-default connmark stroke updown eap-mschapv2 xauth-generic counters
Listening IP addresses:
  192.168.217.129
Connections:
left-to-right:  192.168.217.129 ... 192.168.217.130  IKEv2
left-to-right:   local:  [192.168.217.129] uses pre-shared key authentication
left-to-right:   remote: [192.168.217.130] uses pre-shared key authentication
left-to-right:   child:  192.168.217.129/32 === 192.168.217.130/32 TUNNEL
Security Associations (1 up, 0 connecting):
left-to-right[2]: ESTABLISHED 43 seconds ago, 192.168.217.129[192.168.217.129] ... 192.168.217.130[192.168.217.130]
left-to-right[2]: IKEv2 SPIs: 82b3ff6dd6f204fd_i 6d1bd32f6fe8315b_r*, pre-shared key reauthentication in 2 hours
left-to-right[2]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
left-to-right{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c72b49eb_i c32476fe_o
left-to-right{2}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 45 minutes
left-to-right{2}:   192.168.217.129/32 === 192.168.217.130/32
```

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo ipsec up left-to-right
initiating IKE_SA left-to-right[1] to 192.168.217.130
generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
sending packet: from 192.168.217.129[500] to 192.168.217.130[500] (1208 bytes)
received packet: from 192.168.217.130[500] to 192.168.217.129[500] (472 bytes)
parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
selected proposal: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
authentication of '192.168.217.129' (myself) with pre-shared key
establishing CHILD_SA left-to-right{1}
generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr AUTH SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP)
]
sending packet: from 192.168.217.129[4500] to 192.168.217.130[4500] (432 bytes)
received packet: from 192.168.217.130[4500] to 192.168.217.129[4500] (240 bytes)
parsed IKE_AUTH response 1 [ IDr AUTH SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) ]
authentication of '192.168.217.130' with pre-shared key successful
peer supports MOBIKE
IKE_SA left-to-right[1] established between 192.168.217.129[192.168.217.129] ... 192.168.217.130[192.168.217.130]
scheduling reauthentication in 9726s
maximum IKE_SA lifetime 10266s
selected proposal: ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ
CHILD_SA left-to-right{1} established with SPIs c7c98440_i c9f1eb1b_o and TS 192.168.217.129/32 === 192.168.217.130/32
connection 'left-to-right' established successfully
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.217.130
PING 192.168.217.130 (192.168.217.130) 56(84) bytes of data.
64 bytes from 192.168.217.130: icmp_seq=1 ttl=64 time=0.772 ms
64 bytes from 192.168.217.130: icmp_seq=2 ttl=64 time=0.724 ms
64 bytes from 192.168.217.130: icmp_seq=3 ttl=64 time=0.806 ms
64 bytes from 192.168.217.130: icmp_seq=4 ttl=64 time=0.754 ms
64 bytes from 192.168.217.130: icmp_seq=5 ttl=64 time=0.808 ms
64 bytes from 192.168.217.130: icmp_seq=6 ttl=64 time=0.559 ms
```