

# **VPN Example - IPSec**

# **IPSec** Topology



## **IPSec Server configuration**

1. Open web management page. Click "Services"  $\rightarrow$  "VPN" at the left navigation bar.

伊林思科技有限公司 E-Lins Technology Co.,Limited

VPN	Examp	le -	IPSec
-----	-------	------	-------

stem vices IPSec IPSec IPSec IPSec IPSec ICConfiguration IKEv1-Main  IKEv1-Main IKEv1-Main  IKEv1-Main  IKEv1-Main  IKEv1-Main  IKEv1-Main	
IPSec       MP Check     IPSec Configuration       RRP     Enable       ailover     Exchange mode       NMP     IKEv1-Main       TU     Authentication method       PS     Remote VPN endpoint       PN     Local VPN endpoint	
CMP Check     IPSec Configuration       RRP     Enable       ailover     Enable       NMP     Exchange mode       TU     Authentication method       PS     Remote VPN endpoint       PN     Local VPN endpoint	
RRP     Enable       ailover     Exchange mode       NMP     IKEv1-Main       TU     Authentication method       PS     Remote VPN endpoint       PN     Local VPN endpoint	
Bailover     Exchange mode     IKEv1-Main       NMP     IKEv1-Main     •       TU     Authentication method     Server       PS     Remote VPN endpoint     •       PN     Local VPN endpoint     •	
NMP     Interviewant       TU     Authentication method       PS     Remote VPN endpoint       PN     Local VPN endpoint	
TU     Authentication method     Server       PS     Remote VPN endpoint     *       PN     Local VPN endpoint     *	
PS Remote VPN endpoint	
MS Local VPN endpoint	
PN Local VPN endpoint	
DNS Breshared Keys	
onnect Radio Module	
work Perfect Forward Secrecy Enable *	
out	
None *	
DPD delay 30 seco	onds
NAT Texusted	
Enable *	
Local subnet 192.168.1.0/24	
Pomoto subnot	

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



IPSec PPTP L2TP OpenVPN GRE Tunnel

# **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	<b>]</b> ±



#### Phase 1 Proposal

The phase must match with an	other incoming connection	n to establish IPSec			
Encryption algorithm	AES 192	v			
Hash algorithm	MD5	v			
DH group	MODP2048	Ŧ			
Phase 2 Proposal					
The phase must match with an	other incoming connection	n to establish IPSec			
Encryption algorithm	AES 192	v			
PFS group	MODP2048	T			
Authentic ation	HMAC_MD5	Ŧ			
			Savo & Apply	Savo	Po
			Save & Apply	Save	Re

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

### **IPSec Client configuration**

- 1. Open web management page. Click "Services"  $\rightarrow$  "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.



VPN Example -IPSec

IPSec	PPTP	L2TP	OpenVPN	GRE Tunnel
			oponterit	OT LE T GHING

## **IPSec**

IPSec Configuration		
Enable		
Exchange mode	IKEv2	•
Authentication method	Client	•
Remote VPN endpoint	192.168.5.189	·
Local VPN endpoint	Any	7
Preshared Keys	1234567890	
Perfect Forward Secrecy	Enable	7
DPD action	None	·
DPD delay	30	seconds
NAT Traversal	Enable	·
Local subnet	192.168.1.0/24	
Remote subnet	192.168.2.0/24	<b>*</b>

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	<b>IPSec</b>
----------------	------------	---------	----------	------------	----	-----------	--------------

Encryption algorithm	AES 192	Ŧ	
Hash algorithm	MD5	Ŧ	
DH group	MODP2048	Ŧ	

### Phase 2 Proposal

The phase must match with anoth	er incoming conne	ction to establish IPSec	:		
Encryption algorithm	AES 192				
PFS group	MODP2048	Ŧ			
Authentication	HMAC_MD5	▼			
			Save & Apply	Save	Reset

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

### **IPsec Status**

1. Check IPSec status at client side. Click "Status"  $\rightarrow$  "VPN" at left navigation bar, there is 1 connection is up.

IPSec Status
Reflash
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 80136, tree 12166 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
fd81:607:ba33::1
ipsec_base-ipsec_lan: %any192.168.5.189 IKEv2
<ul> <li>ipsec_base-ipsec_lan: local: uses pre-shared key authentication ipsec_base-ipsec_lan: remote: [192.168.5.189] uses pre-shared key authentication</li> </ul>
ipsec_base-ipsec_lan; child: 192.168.1.0/24 === 192.168.2.0/24 TUNNEL Security Associations (1 up. 0 connecting);
<pre>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</pre>

2. Check IPSec status at server side. Click "Status"  $\rightarrow$  "VPN" at left navigation bar, there is 1 connection is up.

伊林思科技有限公司 E-Lins Technology Co.,Limited

E-Lins

Status	IPSec
Overview	
Network	IPSec Status
Firewall	Reflash
Routes	Status of IKE charon daemon (weakSwan 5.3.3, Linux 3.18.29, mips):
System Log	uptime: 4 minutes, since Sep 13 13:44:15 2016 malloc: shrk 102400, mman 0, used 90792, free 11608
Kernel Log	worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
Reboot Log	loaded plugins: charon aes des sha1 sha2 md5 gmp random nonce hmac stroke kernel-netlink socket-default updown Listening IP addresses:
Realtime Graphs	192 168 5 189
VPN	Connections:
System	ipsec_base-ipsec_lan: %any%any IKEV2 ipsec_base-ipsec_lan: local: uses pre-shared key authentication
Services	ipsec_base-ipsec_lan: remote: uses pre-shared key authentication ipsec_base-ipsec_lan: <u>child: 192.168.2.0/</u> 24 === 192.168.1.0/24 TUNNEL
Network	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)
Logout	ipsec_base-ipsec_lan(1): IKEv2 SPIs: cb5de29815081a7e_i c0f2612ae/ba98a5_r*, pre-sharek key reauthentication in 2 hours ipsec_base-ipsec_lan(1): IKE proposal: AES_CBC_192/IMAC_MD5_96/PRF_HMAC_MD5/MODP_2048 ipsec_base-ipsec_lan(1): INSTALLED, TUNNEL, regid 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: Wsers 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: Wsers 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
```

E-Lins Technology Co.,Limited Address: Rm.33, Unit B, Floor 12, U chuanggu, Xinniu Rd, Minzhi, Longhua, Shenzhen, 518000, China Office Tel: +86 (755) 2923 0581 Email: sales@e-lins.com