

E-Lins Router IPSec Aggressive Mode

This is IPsec settings example for H685/H820/H700/H720/H750 router.

IPSec Server: H685/H820/H700/H720/H750 router, WAN IP: 113.114.209.107, LAN IP: 192.168.8.1, connected device LAN IP: 192.168.8.100;

IPSec Client: H685/H820/H700/H720 router, WAN IP: 113.114.205.243, LAN IP: 10.152.3.100, connected device LAN IP: 10.152.3.101;

Mode: Aggressive

Network Type: Any

Notes: If use IPsec VPN, the VPN Server WAN IP should be visited from Client side without VPN. Otherwise the VPN connection will not be connected.

Server Side

Step 1) Confirm H685/H820/H7X0 Router can be online if it uses WAN CELL Network.

| Internet Configurations | |
|------------------------------|---------------------------------|
| Connected Type | CELL |
| WAN IP Address | 113.114.209.107 |
| Subnet Mask | 255.255.255.255 |
| Default Gateway | 115.168.82.165 |
| Primary Domain Name Server | 202.96.128.86 |
| Secondary Domain Name Server | 220.192.32.103 |
| WAN Speed | download: 0 KBps upload: 0 KBps |
| MAC Address | 08:66:01:03:6B:56 |
| Local Network | |
| Local IP Address | 192.168.8.1 |
| Local Netmask | 255.255.255.0 |
| MAC Address | 08:66:01:03:6B:57 |
| IPSEC Status | |
| Name | Status |
| vpn1 | Active: Active Link: up |
| PPTP Client Status | |
| PPTP | down |
| PPTP IP | |
| PPTP Remote IP | |
| L2TP Client Status | |
| L2TP | down |

Step 2) Configure IPSec.

[open all](#) | [close all](#)

- Router
 - Status
 - Operation Mode
 - DTU
 - Link Backup
 - GPS
 - SMS/Voice
 - VRRP
 - Connect Modem
 - SMS
 - Network Settings
 - VPN
 - Ipsec**
 - PPTP Server
 - PPTP Client
 - L2TP Client
 - Tunnel
- WIFI
- Firewall
- Administration

IPSEC VPN

| IPSEC List | | | | | | |
|--|------|----------------|---------|-----------|---------------|-------------|
| Select | Name | Service Status | Gateway | Interface | Active Status | Link Status |
| <div style="display: flex; justify-content: center; gap: 10px;"> Add/Edit Delete Enable Disable </div> <div style="display: flex; justify-content: center; gap: 10px; margin-top: 5px;"> Restart all Refresh </div> | | | | | | |

IPSEC VPN

| IPSEC List | | | | | | |
|--------------------------|------|----------------|-----------------|-----------|---------------|-------------|
| Select | Name | Service Status | Gateway | Interface | Active Status | Link Status |
| <input type="checkbox"/> | vpn1 | service | 113.114.205.243 | WAN | Active | up |

Add/Edit
Delete
Enable
Disable

Restart all
Refresh

IPSEC VPN

| IPSEC | |
|---------------------|---|
| Name (ID/FQDN) | <input type="text" value="vpn1"/> |
| Service Mode | <input type="text" value="Server"/> |
| Local Network Type | <input type="text" value="Subnet"/> |
| Local IP | <input type="text" value="192.168.8.0"/> : <input type="text" value="24"/> |
| Remote Network Type | <input type="text" value="Subnet"/> |
| Remote IP | <input type="text" value="10.152.3.0"/> : <input type="text" value="24"/> |
| Auth method | <input type="text" value="Pre Shared Key"/> |
| Password | <input type="text" value="••••"/> |
| Interface | <input type="text" value="WAN"/> |
| | <input type="button" value="Advance"/> |

| | |
|---|---|
| NAT Traversal | <input checked="" type="checkbox"/> |
| DPD Check | <input checked="" type="checkbox"/> |
| DPD Interval (sec) | <input type="text" value="60"/> |
| DPD Maximum Failures | <input type="text" value="3"/> |
| Phase1 | |
| Proposal Check | <input type="text" value="obey"/> |
| Encryption Algorithm | <input type="text" value="3DES"/> |
| Hash Algorithm | <input type="text" value="MD5"/> |
| DH Groups | <input type="text" value="modp1024/2"/> |
| Life Time (sec) | <input type="text" value="28800"/> |
| Phase2 | |
| Encryption Algorithm | <input type="text" value="3DES"/> |
| Hash Algorithm | <input type="text" value="MD5"/> |
| DH Groups | <input type="text" value="modp1024/2"/> |
| Life Time (sec) | <input type="text" value="3600"/> |
| Perfect Forward Secrecy | <input type="checkbox"/> |
| <input type="button" value="Apply"/> <input type="button" value="Reset"/> | |

Client Side

Step 1) Confirm H685/H820/H7X0 Router can be online if it uses WAN CELL Network.

| Internet Configurations | |
|------------------------------|---------------------------------|
| Connected Type | CELL |
| WAN IP Address | 113.114.205.243 |
| Subnet Mask | 255.255.255.255 |
| Default Gateway | 183.40.0.1 |
| Primary Domain Name Server | 202.96.128.86 |
| Secondary Domain Name Server | 220.192.32.103 |
| WAN Speed | download: 0 KBps upload: 0 KBps |
| MAC Address | 08:66:01:03:F6:6E |
| Local Network | |
| Local IP Address | 10.152.3.100 |
| Local Netmask | 255.255.255.0 |
| MAC Address | 08:66:01:03:F6:6F |
| IPSEC Status | |
| Name | Status |
| vpn1 | Active: Active Link: up |
| PPTP Client Status | |
| PPTP | down |
| PPTP IP | |
| PPTP Remote IP | |
| L2TP Client Status | |
| L2TP | down |
| L2TP IP | |
| L2TP Remote IP | |

Step 2) Configure IPSec.

IPSEC VPN

| IPSEC List | | | | | | |
|--------------------------|------|----------------|-----------------|-----------|---------------|-------------|
| Select | Name | Service Status | Gateway | Interface | Active Status | Link Status |
| <input type="checkbox"/> | vpn1 | client | 113.114.209.107 | WAN | Active | up |

| IPSEC | |
|---------------------|-------------------|
| Name (ID/FQDN) | vpn1 |
| Service Mode | Client |
| Exchange Mode | Aggressive |
| Gateway | 113.114.209.107 |
| Local Network Type | Subnet |
| Local IP | 10.152.3.0 24 |
| Remote Network Type | Subnet |
| Remote IP | 192.168.8.0 24 |
| Auth method | Pre Shared Key |
| Password | •••• |
| Interface | WAN |
| | Advance |

Apply Reset

| | |
|-------------------------|---|
| NAT Traversal | <input checked="" type="checkbox"/> |
| DPD Check | <input checked="" type="checkbox"/> |
| DPD Interval (sec) | <input type="text" value="60"/> |
| DPD Maximum Failures | <input type="text" value="3"/> |
| Phase1 | |
| Proposal Check | <input type="text" value="obey"/> |
| Encryption Algorithm | <input type="text" value="3DES"/> |
| Hash Algorithm | <input type="text" value="MD5"/> |
| DH Groups | <input type="text" value="modp1024/2"/> |
| Life Time (sec) | <input type="text" value="28800"/> |
| Phase2 | |
| Encryption Algorithm | <input type="text" value="3DES"/> |
| Hash Algorithm | <input type="text" value="MD5"/> |
| DH Groups | <input type="text" value="modp1024/2"/> |
| Life Time (sec) | <input type="text" value="3600"/> |
| Perfect Forward Secrecy | <input type="checkbox"/> |

System Log Indication

```
racoon: INFO: 127.0.0.0[4500] used as isakmp port (fd=16)
racoon: INFO: respond new phase 1 negotiation: 113.114.209.107[500]<=>11
racoon: INFO: begin Aggressive mode.
racoon: INFO: received Vendor ID: RFC 3947
racoon: INFO: received Vendor ID: draft-ietf-ipsec-nat-t-ike-02
racoon: INFO: received Vendor ID: draft-ietf-ipsec-nat-t-ike-02
racoon: INFO: received Vendor ID: draft-ietf-ipsec-nat-t-ike-00
racoon: INFO: received Vendor ID: DPD
racoon: [113.114.205.243] INFO: Selected NAT-T version: RFC 3947
racoon: INFO: Adding remote and local NAT-D payloads.
racoon: [113.114.205.243] INFO: Hashing 113.114.205.243[500] with algo #
racoon: [113.114.209.107] INFO: Hashing 113.114.209.107[500] with algo #
racoon: [113.114.209.107] INFO: Hashing 113.114.209.107[500] with algo #
racoon: INFO: NAT-D payload #0 verified
racoon: [113.114.205.243] INFO: Hashing 113.114.205.243[500] with algo #
racoon: INFO: NAT-D payload #1 verified
racoon: INFO: NAT not detected
racoon: INFO: ISAKMP-SA established 113.114.209.107[500]-113.114.205.243
racoon: [113.114.205.243] INFO: received INITIAL-CONTACT
racoon: INFO: respond new phase 2 negotiation: 113.114.209.107[500]<=>11
racoon: INFO: no policy found, try to generate the policy : 10.152.3.0/2
router: vpn_ipsec:phase1_up-113.114.209.107:500:113.114.205.243:500:vpn1
racoon: INFO: IPsec-SA established: ESP/Tunnel 113.114.209.107[500]->113
racoon: INFO: IPsec-SA established: ESP/Tunnel 113.114.209.107[500]->113
```

Refresh

Clear

Export


```
INFO: 113.114.205.243[4500] used as isakmp port (fd=11)
INFO: 127.0.0.1[500] used for NAT-T
INFO: 127.0.0.1[500] used as isakmp port (fd=12)
INFO: 127.0.0.1[4500] used for NAT-T
INFO: 127.0.0.1[4500] used as isakmp port (fd=13)
INFO: 127.0.0.0[500] used for NAT-T
INFO: 127.0.0.0[500] used as isakmp port (fd=14)
INFO: 127.0.0.0[4500] used for NAT-T
INFO: 127.0.0.0[4500] used as isakmp port (fd=15)
INFO: IPsec-SA request for 113.114.209.107 queued due to no phase1 found
INFO: initiate new phase 1 negotiation: 113.114.205.243[500]<=>113.114.209.107[500]
INFO: begin Aggressive mode.
INFO: received Vendor ID: RFC 3947
INFO: received Vendor ID: DPD
[113.114.209.107] INFO: Selected NAT-T version: RFC 3947
[113.114.205.243] INFO: Hashing 113.114.205.243[500] with algo #1
INFO: NAT-D payload #-1 verified
[113.114.209.107] INFO: Hashing 113.114.209.107[500] with algo #1
INFO: NAT-D payload #0 verified
INFO: NAT not detected
[113.114.209.107] NOTIFY: couldn't find the proper pskey, try to get on
INFO: Adding remote and local NAT-D payloads.
[113.114.209.107] INFO: Hashing 113.114.209.107[500] with algo #1
[113.114.205.243] INFO: Hashing 113.114.205.243[500] with algo #1
INFO: ISAKMP-SA established 113.114.205.243[500]-113.114.209.107[500] spi=1234567890
INFO: initiate new phase 2 negotiation: 113.114.205.243[500]<=>113.114.209.107[500]
[113.114.209.107] INFO: received INITIAL-CONTACT
vpn_ipsec:phase1_up-113.114.205.243:500:113.114.209.107:500:vpn1
INFO: IPsec-SA established: ESP/Tunnel 113.114.205.243[500]->113.114.209.107[500]
```

Test the connection

Step 1) from Client to Server.

```
C:\Users\Sales10>ping 192.168.8.1

正在 Ping 192.168.8.1 具有 32 字节的数据:
来自 192.168.8.1 的回复: 字节=32 时间=743ms TTL=63
来自 192.168.8.1 的回复: 字节=32 时间=128ms TTL=63
来自 192.168.8.1 的回复: 字节=32 时间=162ms TTL=63
来自 192.168.8.1 的回复: 字节=32 时间=155ms TTL=63

192.168.8.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 128ms, 最长 = 743ms, 平均 = 297ms
```

```
C:\Users\Sales10>ping 192.168.8.100

正在 Ping 192.168.8.100 具有 32 字节的数据:
来自 192.168.8.100 的回复: 字节=32 时间=149ms TTL=62
来自 192.168.8.100 的回复: 字节=32 时间=122ms TTL=62
来自 192.168.8.100 的回复: 字节=32 时间=143ms TTL=62
来自 192.168.8.100 的回复: 字节=32 时间=140ms TTL=62

192.168.8.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间<以毫秒为单位>:
    最短 = 122ms, 最长 = 149ms, 平均 = 138ms
```

Step 2) from Server to Client.

```
C:\Documents and Settings\Administrator>ping 10.152.3.100

Pinging 10.152.3.100 with 32 bytes of data:

Reply from 10.152.3.100: bytes=32 time=138ms TTL=63
Reply from 10.152.3.100: bytes=32 time=137ms TTL=63
Reply from 10.152.3.100: bytes=32 time=145ms TTL=63
Reply from 10.152.3.100: bytes=32 time=114ms TTL=63

Ping statistics for 10.152.3.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 114ms, Maximum = 145ms, Average = 133ms
```

```
C:\Documents and Settings\Administrator>ping 10.152.3.101

Pinging 10.152.3.101 with 32 bytes of data:

Reply from 10.152.3.101: bytes=32 time=188ms TTL=62
Reply from 10.152.3.101: bytes=32 time=142ms TTL=62
Reply from 10.152.3.101: bytes=32 time=136ms TTL=62
Reply from 10.152.3.101: bytes=32 time=127ms TTL=62

Ping statistics for 10.152.3.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 127ms, Maximum = 188ms, Average = 148ms
```