# LinEx VPN接入场景使用手册

# 主要功能

1. VPN数据的接入和输出
2. VPN数据在Linex之间路由
3. VPN重复子网的隔离

# 命令行

## IPSec Global Setting

|  |
| --- |
|  |

## IPSec phase1

Parameters of IPSec Phase1 negotiation.

|  |  |  |
| --- | --- | --- |
| property | description | Default value |
| ike-version | ike version :IKEV1/IKEV2 | IKEV1，IKEV2 not support yet |
| local-id | ID of local IKE, must be ipaddr of local IKE，快线网关ipsec监听的地址 | N/A |
| remote-id | ID of remote IKE, must be ipaddr of remote IKE，对端网关的监听地址 | N/A |
| auth\_method | Auth method, currently ,only PSK supported | PSK |
| psksecret | Pre-shared key | N/A |
| remote-port | Listen port of remote IKE | 500 |
| sa-lifetime-byte | Lifetime of Phase1 SA in bytes，定义重新协商的字节数 | 512K |
| sa-lifetime-time | Lifetime of Phase1 SA in seconds，定义重新协商的间隔时间 | 3600 |
| enc-alg | Encrypt algorithoms，第一阶段可选用的加密算法 | 3des\_cbc |
| auth-alg-v1 | Auth algorithoms，第一阶段可选用的认证算法 | Md5 |
| dhgrp | DH Group，用于密钥协商的DH群 | modp768 (GROUP 1) |
| pfs | Perfect forward secrecy，完美向前保密 | disable |
| Psksecret | 预共享秘钥，用来做认证的秘钥 |  |

## IPSec phase2

Parameters of IPSec phase2 negotiation.

|  |  |  |  |
| --- | --- | --- | --- |
| sa-lifetime-time | | IPSec SA lifetime in seconds | 3600 |
| sa-lifetime-byte | | IPSec SA lifetime in bytes | 512K |
| proposal  建议载荷 | protocol | IPsec Protocol:  ESP/AH/IPCOMP | ESP |
| esp-enc-alg | Encrypt algorithoms used in ESP，协商中可选的加密算法 | 3des\_cbc |
| esp-auth-alg | Auth algorithoms used in ESP，协商中可选的认证算法 | hmac\_md5 |
|  |  |  |
|  |  |  |

## IPSec policy

Policy of IPSec, including Phase1 and Phase2 setting.

|  |  |  |
| --- | --- | --- |
| ipsec\_mode | Mode of IPSec:  TUNNEL/TRANSPORT | TUNNEL |
| phase1 | Phase1 setting | N/A |
| Phase2 | Phase2 setting | N/A |
| Sa-local-ip | IP of local IKE | N/A |
| Sa-remote-ip | IP of remote IKE | N/A |

## IPSec flow

Flow filter which defines flows should be en-tunnel.

|  |  |  |
| --- | --- | --- |
| src-addr | source address of flow | N/A |
| dest-addr | Destination address of flow | N/A |
| src-port | Source port of flow | N/A (not support yet) |
| dest-port | Destination port of flow | N/A (not support yet) |
| upper-protocol | L4 protocol | N/A (not support yet) |
| vpnid | VPNID | N/A |
| ipsec-policy | IPsec policy | N/A |
| enable | Enable or disable | enable |

# 应用拓扑



User1和User2是两个用户。

User1有两个子网，10.0.0.0/24和20.0.0.0/24。

User2有三个子网，10.0.0.0/24,20.0.0.0/24,40.0.0.0/24。

Users自己子网之间要通过VPN互访。

其中要解决的问题：

1. 各个子网的接入和输入
2. Linex内网之间根据APP route进行转发
3. User1和User2有重复子网，需要根据VPNID进行隔离。

# 配置示例

## Linex1

### Vpn配置

#### 设置 IKE的服务地址和端口

|  |
| --- |
| config vpn ipsec setting  config ike-listen  edit 1  set ip 192.168.1.1  next  end  end |

#### 配置与User-VPN1和User-VPN2的Phase1协商

|  |
| --- |
| config vpn ipsec phase1  edit 1  set local-id 192.168.1.1  set remote-id 192.168.1.2  set remote-gw 192.168.1.2  set psksecret linex1  next  edit 2  set local-id 192.168.1.1  set remote-id 192.168.1.3  set remote-gw 192.168.1.3  set psksecret linex1  next  end |

#### 配置Phase2的协商

|  |
| --- |
| config vpn ipsec phase2  edit 1  set sa-lifetime-time 60  set sa-lifetime-byte 1024  config proposal  edit sa1  next  end  next  end |

#### 配置policy，关联 phase1于phase2

|  |
| --- |
| config vpn ipsec policy  edit 1  set sa-remote-ip 192.168.1.2  set sa-local-ip 192.168.1.1  set phase1 1  set phase2 1  next  edit 2  set sa-remote-ip 192.168.1.3  set sa-local-ip 192.168.1.1  set phase1 2  set phase2 1  next  end |

#### 配置FLow，定义进入隧道的流量，与相应的policy相关联

|  |
| --- |
| config vpn ipsec flow  edit 2  set src-addr 20.0.0.0/24  set dest-addr 10.0.0.0/24  set ipsec-policy 1  set enable enable  set vpnid 2  next  edit 4  set src-addr 40.0.0.0/24  set dest-addr 10.0.0.0/24  set ipsec-policy 1  set enable enable  set vpnid 2  next  end |

### Approute配置

#### 定义网络中的Linex节点

|  |
| --- |
| config application-route gateway  edit GW\_SELF  set description "predefined self gateway"  set type self  not ipv4 address 0  next  edit linex2  set address 30.0.0.2  next  edit linex3  set address 30.0.0.3  next  end |

#### 定义VPN相关的APP route

|  |
| --- |
| config application-route route  edit 2  set type VPN  set vpnid 3  set destination-network 20.0.0.0/24  set nexthop-gateway linex3  next  edit 1  set type VPN  set vpnid 2  set destination-network 20.0.0.0/24  set nexthop-gateway linex2  next  edit 3  set type VPN  set vpnid 2  set destination-network 40.0.0.0/24  set nexthop-gateway linex3  next  end |

## Linex2

### VPN配置

|  |
| --- |
| config vpn ipsec setting  config ike-listen  edit 1  set ip 192.168.2.1  next  end  end  config vpn ipsec phase1  edit 1  set local-id 192.168.2.1  set remote-id 192.168.2.2  set remote-gw 192.168.2.2  set psksecret linex2  next  end  config vpn ipsec phase2  edit 1  set sa-lifetime-time 60  set sa-lifetime-byte 1024  config proposal  edit sa  next  end  next  end  config vpn ipsec policy  edit 1  set sa-remote-ip 192.168.2.2  set sa-local-ip 192.168.2.1  set phase1 1  set phase2 1  next  end  config vpn ipsec flow  edit 1  set src-addr 10.0.0.0/24  set dest-addr 20.0.0.0/24  set ipsec-policy 1  set enable enable  set vpnid 2  next  edit 2  set src-addr 40.0.0.0/24  set dest-addr 20.0.0.0/24  set ipsec-policy 1  set enable enable  set vpnid 2  next  end |

### APP route 配置

|  |
| --- |
| config application-route gateway  edit GW\_SELF  set description "predefined self gateway"  set type self  not ipv4 address 0  next  edit linex1  set address 30.0.0.1  next  edit linex3  set address 30.0.0.3  next  end  config application-route route  edit 1  set type VPN  set vpnid 2  set destination-network 10.0.0.0/24  set nexthop-gateway linex1  next  edit 2  set type VPN  set vpnid 2  set destination-network 40.0.0.0/24  set nexthop-gateway linex3  next  end |

## Linex3

### VPN配置

|  |
| --- |
| config vpn ipsec setting  config ike-listen  edit 1  set ip 192.168.3.1  next  end  end  config vpn ipsec phase1  edit 1  set local-id 192.168.3.1  set remote-id 192.168.3.3  set remote-gw 192.168.3.3  set psksecret linex3  next  edit 2  set local-id 192.168.3.1  set remote-id 192.168.3.2  set remote-gw 192.168.3.2  set psksecret linex3  next  end  config vpn ipsec phase2  edit 1  set sa-lifetime-time 60  set sa-lifetime-byte 1024  config proposal  edit prop1  next  end  next  end  config vpn ipsec policy  edit 1  set sa-remote-ip 192.168.3.3  set sa-local-ip 192.168.3.1  set phase1 1  set phase2 1  next  edit 2  set sa-remote-ip 192.168.3.2  set sa-local-ip 192.168.3.1  set phase1 2  set phase2 1  next  end  config vpn ipsec flow  edit 1  set src-addr 10.0.0.0/24  set dest-addr 40.0.0.0/24  set ipsec-policy 1  set enable enable  set vpnid 2  next  edit 2  set src-addr 20.0.0.0/24  set dest-addr 40.0.0.0/24  set ipsec-policy 1  set enable enable  set vpnid 2  next  edit 3  set src-addr 10.0.0.0/24  set dest-addr 20.0.0.0/24  set ipsec-policy 2  set enable enable  set vpnid 3  next  end |

### APP Route 配置

|  |
| --- |
| config application-route gateway  edit GW\_SELF  set description "predefined self gateway"  set type self  not ipv4 address 0  next  edit linex1  set address 30.0.0.1  next  edit linex2  set address 30.0.0.2  next  end  config application-route route  edit 1  set type VPN  set vpnid 2  set destination-network 10.0.0.0/24  set nexthop-gateway linex1  next  edit 2  set type VPN  set vpnid 2  set destination-network 20.0.0.0/24  set nexthop-gateway linex2  next  edit 3  set type VPN  set vpnid 3  set destination-network 10.0.0.0/24  set nexthop-gateway linex1  next  end |