VPN配置说明

版本信息：

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 更新者 | 修订日期 | 说明 |
| 1.0 | 缪璐璟 | 2015/01/08 | 创建 |

目 录

[1 快线网关说明 3](#_Toc409112481)

[1.1 Ipsec说明 3](#_Toc409112482)

[1.2 快线网关字段说明 3](#_Toc409112483)

[1.2.1 IPSec phase1 3](#_Toc409112484)

[1.2.2 IPSec phase2 4](#_Toc409112485)

[1.2.3 IPSec policy 4](#_Toc409112486)

[1.2.4 IPSec flow 4](#_Toc409112487)

[2 应用拓扑 5](#_Toc409112488)

[3 配置说明 6](#_Toc409112489)

[3.1 Linex1配置 6](#_Toc409112490)

[3.1.1 Vpn配置 6](#_Toc409112491)

[3.1.2 Approute配置 8](#_Toc409112492)

[3.2 Linex2配置 10](#_Toc409112493)

[3.2.1 Vpn配置 10](#_Toc409112494)

[3.2.2 Approute配置 12](#_Toc409112495)

[3.3 Linex3配置 13](#_Toc409112496)

[3.3.1 Vpn配置 13](#_Toc409112497)

[3.3.2 Approute配置 15](#_Toc409112498)

# 快线网关说明

## Ipsec说明

IPsec 协商，包括两个阶段，第一个阶段，做认证，并协商出一组算法和秘钥，为第二个阶段的协商做保护。第二个阶段的协商，用第一阶段的协商结果加密，协商出真正用于加密数据的算法和秘钥。第一阶段的协商参数在 ph1中定义，第二阶段的协商参数在ph2中定义。

第一阶段协商成功后，协商结果会以一个SA的方式保存下来。这个SA不是永久不变的。为了安全起见，会每隔一段时间，或者每加密一定字节数之后，重新协商。

IPsec 支持两种子协议，ESP和AH。 隧道模式一般都是采用ESP。所以这里默认就是ESP。ESP协议包含了加密和认证，esp\_enc和esp\_auth分别是协商中可选的加密算法和认证算法。AH协议只包含了认证，不加密。 Ah \_auth是可选的认证算法。IPsec还支持数据包压缩，即 IPCOMP。一般不启用。Ipcomp\_alg即IP压缩的算法。

## 快线网关字段说明

### IPSec phase1

|  |  |  |
| --- | --- | --- |
| **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

|  |  |  |  |
| --- | --- | --- | --- |
| **property** | | **description** | **Default value** |
| 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

|  |  |  |
| --- | --- | --- |
| **property** | **description** | **Default value** |
| 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

|  |  |  |
| --- | --- | --- |
| **property** | **description** | **Default value** |
| 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，192.168.1.0/24和192.168.2.0/24。

User2有三个子网，192.168.1.0/24，192.168.2.0/24，192.168.3.0/24。

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。

# 配置说明

## Linex1配置

### 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 115.236.57.114  next  end  end |

#### 配置Phase1协商

|  |
| --- |
| config vpn ipsec phase1  edit 1  set local-id 115.236.57.114  set remote-id 115.236.57.109  set remote-gw 115.236.57.109  set psksecret linex1  next  edit 2  set local-id 115.236.57.114  set remote-id 115.236.57.110  set remote-gw 115.236.57.110  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 1  set protocol esp  set esp-enc-alg 3des\_cbc  set esp-auth-alg hmac\_md5  next  end  next  end |

#### 配置policy，关联 phase1于phase2

|  |
| --- |
| config vpn ipsec policy  edit 1  set ipsec\_mode tunnel  set sa-remote-ip 115.236.57.109  set sa-local-ip 115.236.57.114  set phase1 1  set phase2 1  next  edit 2  set ipsec\_mode tunnel  set sa-remote-ip 115.236.57.110  set sa-local-ip 115.236.57.114  set phase1 2  set phase2 1  next  end |

#### 配置FLow，与相应的policy相关联

|  |
| --- |
| config vpn ipsec flow  edit net1\_net2  set src-addr 192.168.2.0/24  set dest-addr 192.168.1.0/24  set ipsec-policy 1  set enable enable  set vpnid 1  next  edit net2\_net2  set src-addr 192.168.2.0/24  set dest-addr 192.168.1.0/24  set ipsec-policy 2  set enable enable  set vpnid 2  next  edit net2\_net3  set src-addr 192.168.3.0/24  set dest-addr 192.168.1.0/24  set ipsec-policy 2  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  unset address  next  edit JXLT-10.1.24.202\_10.1.17.202  unset description  set type peer  set address 10.1.17.202  next  edit ZJHZ-10.1.24.203\_10.1.17.203  unset description  set type peer  set address 10.1.17.203  next  end |

#### 定义VPN相关的APP route

|  |
| --- |
| config application-route route  edit 204  set type VPN  set vpnid 1  set destination-network 192.168.2.0/24  set nexthop-gateway JXLT-10.1.24.202\_10.1.17.202  next  edit 205  set type VPN  set vpnid 1  set destination-network 192.168.1.0/24  set nexthop-gateway GW\_SELF  next  edit 221  set type VPN  set vpnid 2  set destination-network 192.168.1.0/24  set nexthop-gateway GW\_SELF  next  edit 222  set type VPN  set vpnid 2  set destination-network 192.168.2.0/24  set nexthop-gateway ZJHZ-10.1.24.203\_10.1.17.203  next  edit 223  set type VPN  set vpnid 2  set destination-network 192.168.3.0/24  set nexthop-gateway JXLT-10.1.24.202\_10.1.17.202  next  edit 226  set type forward  set forward-mark 5  set nexthop-gateway ZJHZ-10.1.24.203\_10.1.17.203  next  edit 231  set type forward  set forward-mark 13  set nexthop-gateway JXLT-10.1.24.202\_10.1.17.202  next  end |

## Linex2配置

### 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 101.69.204.168  next  end  end |

#### 配置Phase1协商

|  |
| --- |
| config vpn ipsec phase1  edit 1  set local-id 101.69.204.168  set remote-id 115.236.57.112  set remote-gw 115.236.57.112  set psksecret linex1  next  edit 2  set local-id 101.69.204.168  set remote-id 115.236.57.113  set remote-gw 115.236.57.113  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 1  set protocol esp  set esp-enc-alg 3des\_cbc  set esp-auth-alg hmac\_md5  next  end  next  end |

#### 配置policy，关联 phase1于phase2

|  |
| --- |
| config vpn ipsec policy  edit 1  set sa-remote-ip 115.236.57.112  set sa-local-ip 101.69.204.168  set phase1 1  set phase2 1  next  edit 2  set sa-remote-ip 115.236.57.113  set sa-local-ip 101.69.204.168  set phase1 2  set phase2 1  next  end |

#### 配置FLow，与相应的policy相关联

|  |
| --- |
| config vpn ipsec flow  edit 1  set src-addr 192.168.1.0/24  set dest-addr 192.168.2.0/24  set ipsec-policy 1  set enable enable  set vpnid 1  next  edit 2  set src-addr 192.168.2.0/24  set dest-addr 192.168.3.0/24  set ipsec-policy 2  set enable enable  set vpnid 2  next  edit 3  set src-addr 192.168.1.0/24  set dest-addr 192.168.3.0/24  set ipsec-policy 2  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  unset address  next  edit XSDX-10.1.24.201\_10.1.17.201  unset description  set type peer  set address 10.1.17.201  next  edit ZJHZ-10.1.24.203\_10.1.17.203  unset description  set type peer  set address 10.1.17.203  next  end |

#### 定义VPN相关的APP route

|  |
| --- |
| config application-route route  edit 206  set type VPN  set vpnid 1  set destination-network 192.168.2.0/24  set nexthop-gateway GW\_SELF  next  edit 207  set type VPN  set vpnid 1  set destination-network 192.168.1.0/24  set nexthop-gateway XSDX-10.1.24.201\_10.1.17.201  next  edit 224  set type VPN  set vpnid 2  set destination-network 192.168.1.0/24  set nexthop-gateway XSDX-10.1.24.201\_10.1.17.201  next  edit 225  set type VPN  set vpnid 2  set destination-network 192.168.2.0/24  set forward-mark 5  set nexthop-gateway XSDX-10.1.24.201\_10.1.17.201  next  edit 227  set type VPN  set vpnid 2  set destination-network 192.168.3.0/24  set nexthop-gateway GW\_SELF  next  end |

## Linex3配置

### 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 113.215.9.231  next  end  end |

#### 配置Phase1协商

|  |
| --- |
| config vpn ipsec phase1  edit 1  set local-id 113.215.9.231  set remote-id 115.236.57.111  set remote-gw 115.236.57.111  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 1  set protocol esp  set esp-enc-alg 3des\_cbc  set esp-auth-alg hmac\_md5  next  end  next  end |

#### 配置policy，关联 phase1于phase2

|  |
| --- |
| config vpn ipsec policy  edit 1  set ipsec\_mode tunnel  set sa-remote-ip 115.236.57.111  set sa-local-ip 113.215.9.231  set phase1 1  set phase2 1  next  end |

#### 配置FLow，与相应的policy相关联

|  |
| --- |
| config vpn ipsec flow  edit 1  set src-addr 192.168.1.0/24  set dest-addr 192.168.2.0/24  set ipsec-policy 1  set enable enable  set vpnid 2  next  edit 2  set src-addr 192.168.3.0/24  set dest-addr 192.168.2.0/24  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 XSDX-10.1.24.201\_10.1.17.201  set address 10.1.17.201  next  edit JXLT-10.1.24.202\_10.1.17.202  set address 10.1.17.202  next  end |

#### 定义VPN相关的APP route

|  |
| --- |
| config application-route route  edit 228  set type VPN  set vpnid 2  set destination-network 192.168.1.0/24  set nexthop-gateway XSDX-10.1.24.201\_10.1.17.201  next  edit 229  set type VPN  set vpnid 2  set destination-network 192.168.2.0/24  set nexthop-gateway GW\_SELF  next  edit 230  set type VPN  set vpnid 2  set destination-network 192.168.3.0/24  set forward-mark 13  set nexthop-gateway XSDX-10.1.24.201\_10.1.17.201  next  end |