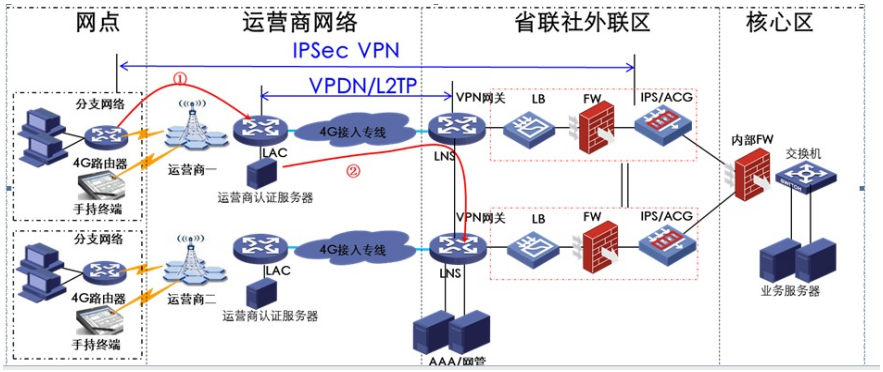
WinXP通过M9000进行l2tp over ipsec拨号，中间串LB进行拨号流量负载，拨号失败

outbound链路负载均衡 L2TP IPSec 酉海华 2016-01-27 发表

某局点2台v7防火墙做l2tp over ipsec VPN sever，中间串L1000-S设备作为vpn负载均衡，目前测试发现pc winxp拨l2tp over ispec VPN无法拨通，win7和手机拨入正常。



IKE诊断信息：

*Mar 7 18:46:57:616 2016 FW-1 IKE/7/EVENT: -Context=1; Received message from ipsec.

*Mar 7 18:46:57:616 2016 FW-1 IKE/7/EVENT: -Context=1; vrf = 0, src = 11.0.224.18, dst = 192.168.199.164/4500

IPsec SA state changed from IKE_P2_STATE_INIT to IKE_P2_STATE_GETSP.

*Mar 7 18:46:57:616 2016 FW-1 IKE/7/ERROR: -Context=1; vrf = 0, src = 11.0.224.18, dst = 192.168.199.164/4500

Failed to get IPsec policy for phase 2 responder. Delete IPsec SA.

*Mar 7 18:46:57:616 2016 FW-1 IKE/7/ERROR: -Context=1; vrf = 0, src = 11.0.224.18, dst = 192.168.199.164/4500

Failed to negotiate IPsec SA.

*Mar 7 18:46:57:616 2016 FW-1 IKE/7/EVENT: -Context=1; Delete IPsec SA.

*Mar 7 18:46:57:617 2016 FW-1 IKE/7/PACKET: -Context=1; vrf = 0, src = 11.0.224.18, dst = 192.168.199.164/4500

Encrypt the packet.

*Mar 7 18:46:57:618 2016 FW-1 IKE/7/PACKET: -Context=1; vrf = 0, src = 11.0.224.18, dst = 192.168.199.164/4500

Construct notification packet: INVALID_ID_INFORMATION.

1、默认情况下，Windows XP SP2 不再支持与位于网络地址转换器后面的服务器的 IPsec NAT-T 安全关联。因此，如果虚拟专用网络 (VPN) 服务器位于网络地址转换器的后面，则在默认情况下，基于 Windows XP SP2 的 VPN 客户端无法与 VPN 服务器进行 L2TP/IPsec 连接。要改变运行 Windows XP SP2 的计算机的 IPsec NAT-T 行为，必须创建 AssumeUDPEncapsulationContextOnSendRule 注册表值。

2、缺少针对Winxp的IPSec安全提议：采用ESP协议，ESP验证算法采用MD5,ESP加密算法采用3DES。

```
ipsec transform-set 1
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-192
 esp authentication-algorithm sha1
#
ipsec transform-set 2
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec transform-set 3
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha1
#
ipsec transform-set 4
```

```
 encapsulation-mode transport
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set 5
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set 6
 encapsulation-mode transport
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec policy-template 1 1
 transform-set 1 2 3 4 6
 security acl 3001
 ike-profile 1
#
ipsec policy-template 2 1
 transform-set 5
 ike-profile 2
 reverse-route dynamic
#
```

1、修改注册表：
在 Windows 桌面上，单击“开始”，单击“运行”，键入“regedit.exe”，然后单击“确定”。 在“注册表编辑”的控制台树中，打开下列注册表项：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPSEC。在“编辑”菜单上，单击“添加值，然后添加下列值：值名：AssumeUDPEncapsulationContextOnSendRule 数据类型：REG_DWORD 数据值：2

- 值 0（默认）将 Windows 配置为无法建立与位于网络地址转换器后面的服务器的安全关联。
- 值 1 将 Windows 配置为可以建立与位于网络地址转换器后面的服务器的安全关联。
- 值 2 将 Windows 配置为可以在服务器和基于 Windows XP SP2 的客户机都位于网络地址转换器后面时建立安全关联。

2、创建一个ipsec tranform-set，并在ipsec policy-template 1 1中引用。

```
#
ipsec transform-set 7
 encapsulation-mode transport
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
```

不对PC客户端兼容性不一样，根据典配完成VPN配置后，若拨号错误，可根据具体的错误值进行对应修改。