SecPath F1000-E-SI 防火墙的策略路由在ipsec over l2tp组网方案中的应用

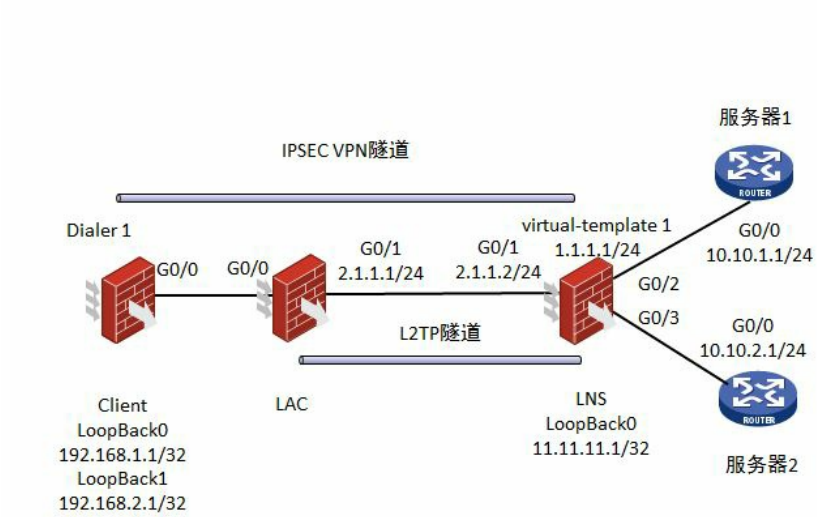
L2TP IPSec 李聪 2016-09-12 发表

一、 组网需求：

如图所示，三台防火墙分别是客户端、LAC、LNS。目前的需求是数据经过客户端防火墙之后，client防火墙会向LAC防火墙拨号，然后触发LAC防火墙和LNS防火墙建立协商L2TP隧道。Client防火墙从LNS防火墙获取一个拨号地址，此时可以看作client到LNS逻辑上是连接的。目前对于数据安全的考虑，在client的dialer接口以及LNS的VT虚接口上启用ipsec vpn协商保护数据。本案例采用野蛮模式的方式建立ipsec vpn，LNS侧使用策略模板方式建立ipsec vpn。由于client侧有两个内网网段，需要在LNS上面的VT虚接口上启用策略路由使内网网段192.168.1.0/24只能访问服务器网段10.10.1.0/24，网段192.168.2.0/24只能访问服务器网段10.10.2.0/24。

本配置案例使用的防火墙均为SecPath F1000-E-SI，版本为Version 5.20, Release 3734P09。

二、 组网图：



三、 配置步骤：

设备SecPath F1000-E-SI，版本为Version 5.20, Release 3734P09。

1. 配置client

防火墙需要将接口加入到安全域，然后开放相关的安全域的域间策略的配置。域间策略的配置略。

配置设备名称为client

sysname client

配置loopback0以及loopback1接口地址，分别表示本地设备的内网网段

[client]interface LoopBack 0

[client-LoopBack0]ip address 192.168.1.1 32

[client-LoopBack0]quit

[client]interface LoopBack 1

[client-LoopBack0]ip address 192.168.2.1 32

[client-LoopBack0]quit

配置本端安全网关设备名称。

system-view

[client] ike local-name client

配置ipsec vpn保护的数据流。

[client] acl number 3101

定义去往服务器保护的数据流。

[client-acl-adv-3101] rule 0 permit ip source 192.168.0.0 0.0.255.255 destination 10.10.0.0 0.0.255.25
5

定义去往lns设备本地网段保护的数据流。

[client-acl-adv-3101] rule 1 permit ip source 192.168.0.0 0.0.255.255 destination 11.11.11.0 0.0.0.255

[client-acl-adv-3101] quit

配置IKE安全提议。

[client] ike proposal 1

[client-ike-proposal-1] authentication-algorithm sha

[client-ike-proposal-1] authentication-method pre-share

[client-ike-proposal-1] encryption-algorithm 3des-cbc

[client-ike-proposal-1] dh group2

配置IKE对等体peer。

[client] ike peer peer

[client-ike-peer-peer] exchange-mode aggressive

[client-ike-peer-peer] proposal 1

[client-ike-peer-peer] pre-shared-key simple 123456

[client-ike-peer-peer] id-type name

[client-ike-peer-peer] remote-name lns

[client-ike-peer-peer] remote-address 1.1.1.1

[client-ike-peer-peer] quit

创建IPsec安全提议tran1。

[client] ipsec transform-set tran1

[client-ipsec-transform-set-tran1] encapsulation-mode tunnel

[client-ipsec-transform-set-tran1] transform esp

[client-ipsec-transform-set-tran1] esp encryption-algorithm 3des

[client-ipsec-transform-set-tran1] esp authentication-algorithm sha1

[client-ipsec-transform-set-tran1] quit

创建IPsec安全策略policy并指定通过IKE协商建立SA。

[client] ipsec policy policy 1 isakmp

配置IPsec安全策略policy引用IKE对等体peer。

[client-ipsec-policy-isakmp-policy-1] ike-peer peer

配置IPsec安全策略policy引用访问控制列表3101。

[client-ipsec-policy-isakmp-policy-1] security acl 3101

配置IPsec安全策略policy引用IPsec安全提议tran1。

[client-ipsec-policy-isakmp-policy-1] transform-set tran1

[client-ipsec-policy-isakmp-policy-1] quit

配置拨号访问控制列表。

[client] dialer-rule 1 ip permit

创建Dialer0，使用由lns分配的用户名和密码进行拨号，并且在dialer接口下面调用ipsec policy。

[client] interface dialer 0

[client-Dialer0] link-protocol ppp

[client-Dialer0] ppp pap local-user test password simple 123456

[client-Dialer0] ip address ppp-negotiate

[client-Dialer0] dialer user test

[client-Dialer0] dialer-group 1

[client-Dialer0] dialer bundle 1

[client-Dialer0] ipsec policy policy

配置PPPoE会话。

[client] interface GigabitEthernet0/0

[client-GigabitEthernet0/0] pppoe-client dial-bundle-number 1

配置到lns本地网段以及服务器的默认路由。

[client] ip route-static 0.0.0.0 0 dialer 0

2. 配置lac

防火墙需要将接口加入到安全域，然后开放相关的安全域的域间策略的配置。域间策略的配置略。

配置设备名称为lac

sysname lac

启用L2TP服务，并设置一个L2TP组。

system-view

[lac] l2tp enable

[lac] l2tp-group 1

配置LAC侧本端名称，配置对端LNS的IP地址。

[lac-l2tp1] tunnel name lac

[lac-l2tp1] start l2tp ip 2.1.1.2 domain system

启用通道验证并设置通道验证密钥。

[lac-l2tp1] tunnel authentication

[lac-l2tp1] tunnel password simple 123456

[lac-l2tp1] quit

配置virtual-template接口及PPP验证方式为PAP。

[lac] interface virtual-template 1

[lac-Virtual-Template1] ppp authentication-mode pap

[lac-Virtual-Template1] quit

配置G0/1口的ip地址。

[lac] interface GigabitEthernet0/1

[lac-GigabitEthernet0/1] ip address 2.1.1.1 24

[lac-GigabitEthernet0/1]quit

配置pppoe-server并将virtual-template接口绑定在G0/0口。

[lac] interface GigabitEthernet0/0

[lac-GigabitEthernet0/0]pppoe-server bind Virtual-Template 1

[lac-GigabitEthernet0/0]quit

创建本地用户，配置用户名、密码及服务类型。

[lac] local-user test

[lac-luser-test] password simple 123456

[lac-luser-test] service-type ppp

配置默认路由。

[lac] ip route-static 0.0.0.0 0 2.1.1.2

3. 配置lns

防火墙需要将接口加入到安全域，然后开放相关的安全域的域间策略的配置。域间策略的配置略。

配置设备名称为lns

sysname lns

配置loopback0接口地址，表示本地设备的内网网段。

[lns]interface LoopBack 0

[lns-LoopBack0]ip address 11.11.11.1 32

[lns-LoopBack0]quit

配置G0/1、G0/2、G0/3口的ip地址。

[lns] interface GigabitEthernet0/1

[lns-GigabitEthernet0/1] ip address 2.1.1.2 24

[lns-GigabitEthernet0/1] interface GigabitEthernet0/2

[lns-GigabitEthernet0/2] ip address 10.10.1.2 24

[lns-GigabitEthernet0/2] interface GigabitEthernet0/3

[lns-GigabitEthernet0/3] ip address 10.10.2.2 24

[lns-GigabitEthernet0/3]quit

配置本端安全网关设备名称。

[lns] ike local-name lns

配置ipsec vpn保护的数据流。

[lns] acl number 3101

[lns-acl-adv-3101] rule 0 permit ip source 10.10.0.0 0.0.255.255 destination 192.168.0.0 0.0.255.255

[lns-acl-adv-3101] rule 1 permit ip source 11.11.11.0 0.0.0.255 destination 192.168.0.0 0.0.255.255

[lns-acl-adv-3101] quit

配置IKE安全提议。

[lns] ike proposal 1

[lns-ike-proposal-1] authentication-algorithm sha

[lns-ike-proposal-1] authentication-method pre-share

[lns-ike-proposal-1] encryption-algorithm 3des-cbc

[lns-ike-proposal-1] dh group2

配置IKE对等体peer。

[lns] ike peer peer

[lns-ike-peer-peer] exchange-mode aggressive

[lns-ike-peer-peer] proposal 1

[lns-ike-peer-peer] pre-shared-key simple 123456

[lns-ike-peer-peer] id-type name

[lns-ike-peer-peer] remote-name client

[lns-ike-peer-peer] local-address 1.1.1.1

[lns-ike-peer-peer] local-name lns

[lns-ike-peer-peer] quit

创建IPsec安全提议tran1。

[lns] ipsec transform-set tran1

[lns-ipsec-transform-set-tran1] encapsulation-mode tunnel

[lns-ipsec-transform-set-tran1] transform esp

[lns-ipsec-transform-set-tran1] esp encryption-algorithm 3des

[lns-ipsec-transform-set-tran1] esp authentication-algorithm sha1

[lns-ipsec-transform-set-tran1] quit

创建一个IKE协商方式的IPsec安全策略模板，名称为test，顺序号为1。

[lns] ipsec policy-template test 1

配置IPsec安全策略policy模板引用IKE对等体peer。

[lns-ipsec-policy-template-test-1] ike-peer peer

配置IPsec安全策略policy模板引用访问控制列表3101。

[lns-ipsec-policy-template-test-1] security acl 3101

指定引用的安全提议为tran1。

[lns-ipsec-policy-template-test-1] transform-set tran1

[lns-ipsec-policy-template-test-1] quit

将IPsec模板和策略绑定。

[lns]ipsec policy policy 1 isakmp template test

创建本地用户，配置用户名、密码及服务类型。

[lns] local-user test

[lns-luser-test] password simple 123456

[lns-luser-test] service-type ppp

配置匹配192.168.1.0/24的网段流量。

[lns] acl number 3102

[lns-acl-adv-3102] rule 0 permit ip source 192.168.1.0 0.0.0.255

[lns-acl-adv-3102] quit

配置匹配192.168.2.0/24的网段流量。

[lns] acl number 3103

[lns-acl-adv-3103] rule 0 permit ip source 192.168.2.0 0.0.0.255

[lns-acl-adv-3103] quit

配置策略路由节点，源网段192.168.1.0/24访问10.10.1.0/24的策略路由。

[lns] policy-based-route aaa permit node 10

[lns-pbr-aaa-10] if-match acl 3102

[lns-pbr-aaa-10] apply ip-address next-hop 10.10.1.1

[lns-pbr-aaa-10] quit

配置策略路由节点，源网段192.168.2.0/24访问10.10.2.0/24的策略路由。

[lns] policy-based-route aaa permit node 20

[lns-pbr-aaa-20] if-match acl 3103

[lns-pbr-aaa-20] apply ip-address next-hop 10.10.2.1

[lns-pbr-aaa-20] quit

配置L2TP VPN的用户地址池。

[lns] domain system

[lns-isp-system] authentication ppp local

[lns-isp-system] ip pool 1 1.1.1.2 1.1.1.254

[lns-isp-system] quit

配置虚拟模板接口Virtual-Template1的相关信息，引用ipsec policy并且调用策略路由实现client侧不同网段访问不同的服务器网段。

[lns] interface virtual-template 1

[lns-virtual-template1] ip address 1.1.1.1 255.255.255.0

[lns-virtual-template1] remote address pool 1

[lns-virtual-template1] ppp authentication-mode pap

[lns-virtual-template1] ip policy-based-route aaa

[lns-virtual-template1] ipsec policy policy

[lns-virtual-template1] quit

启用L2TP服务，并设置一个L2TP组。

[lns] l2tp enable

[lns] l2tp-group 1

配置LNS侧本端名称及接收的通道对端名称。

[lns-l2tp1] tunnel name lns

[lns-l2tp1] allow l2tp virtual-template 1 remote lac

启用通道验证并设置通道验证密钥。

[lns-l2tp1] tunnel authentication

[lns-l2tp1] tunnel password simple 123456

[lns-l2tp1] quit

配置去往client网段的静态路由。

[lns] ip route-static 192.168.0.0 16 virtual-template 1

四、 配置关键点：

1. 按照组网图配置各个设备的接口地址以及路由保证网络通畅。接口都加入安全域并且放开相关区域的域间策略。

2. Client与lns之间建立ipsec vpn，ipsec vpn是在l2tp之上的，因此本例采用的是ipsec over l2tp vpn。Client端在dialer接口上调用ipsec policy，而lns端则是在virtual-template 1接口上面调用ipsec policy。

3. 本配置案例难点在于能否在virtual-template 1接口上面调用策略路由实现不同的源网段访问不同的目的网段。经过验证，仅是在配置l2tp的时候，在virtual-template 1接口上调用策略路由能够实现需求。进一步的验证表明即使加ipsec vpn的配置，在virtual-template 1上面调用策略路由也能够实现需求。

4. 本案例lns端采用野蛮模式建立ipsec vpn，因为不能确定client分配到的ip地址，因此lns侧采用模板的方式建立ipsec vpn。

5. 本案例流量到了lns设备上面之后会从virtual-template 1解封装，然后解封装ipsec vpn的流量，然后根据virtual-template 1上面配置的策略路由进行选路。

6. 模拟服务器1和服务器2上面的路由器分别需要配置回指给client端网段的静态路由。