野蛮模式下如何使中心能够主动访问分支业务数据

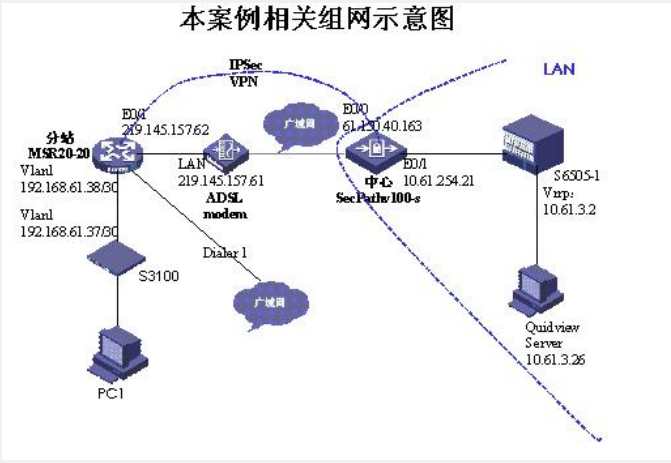
张瑞 2007-05-18 发表

IPSec VPN野蛮模式下分支如何主动建立连接

一、组网介绍：

中心SecPath v100-s与分站MSR20-20通过广域网互联，分站侧通过固定地址219.145.157.62与ADSL Modem互联，modem的互联地址为219.145.157.61，在分站MSR20-20与中心SecPath v100-s之间应用野蛮模式建立IPSec VPN隧道，允许私网10.61.0.0网段的数据进行互访；同时MSR20-20通过另外一条ADSL拨号线路（Dialer1）连接到公网，供内部用户访问Internet。其它设备与IP如图中所示。

二、组网图：



三、 问题描述：

正常情况下，在IPSec VPN的野蛮模式下，只有当分站主动发起访问私网数据的请求，才会触发ike协商进而建立VPN隧道，在本案例中，中心作为信息存储中心，需要周期性的从分站读取业务数据。由于分站可能是无人值守的台站，而设备可能由于各种原因而重新启动，在这种情况下，中心将无法主动触发建立VPN的链接，进而无法获取分站数据。而各个分站均只能以野蛮模式接入。

四、 过程分析：

对于该需求，您的第一反应可能是IPSec VPN不是有DPD（Dead Peer Detection，对等体存活检测）吗?

经过一番测试发现，在正常情况下（两端的设备均未重启），DPD可以起到VPN的保持作用。但是如果分站的设备重新启动后，则分站不会主动触发建立VPN，中心虽有访问分站的需求，无奈协议限制，也无法触发建立VPN，从而无法访问分站的业务数据。

于是我们想到了Info-Center，因为只要在路由器UP的情况下有从分站到中心的业务数据就可以触发VPN的建立，而Info-Center正好具备这一特性，在迅速的配置完成之后，发现在设备重启后依然无法在短时间内重新触发建立VPN。

后来还想到利用BIMS报文来触发VPN拨号，但是还是以失败告终。

四、 解决方案：

最后想到了NTP（Network Time Protocol，网络时间协议），该协议的基本原理是对网络内所有具有时钟的设备进行时钟同步，使网络内所有设备的时钟保持一致，从而使设备能够提供基于统一时间的多种应用。

对于运行NTP的本地系统，既可以接受来自其他时钟源的同步，又可以作为时钟源同步其他的时钟，并且可以和其他设备互相同步。

设备可以采用多种NTP工作模式进行时间同步：

服务器/客户端模式

在服务器/客户端模式中，客户端向服务器发送时钟同步报文，报文中的Mode字段设置为3（客户模式）。服务器端收到报文后会自动工作在服务器模式，并发送应答报文，报文中的Mode字段设置为4（服务器模式）。客户端收到应答报文后，进行时钟过滤和选择，并同步到优选的服务器。

在该模式下，客户端能同步到服务器，而服务器无法同步到客户端。

对等体模式
在对等体模式中，主动对等体和被动对等体之间首先交互Mode字段为3（客户端模式）和4（服务器模式）的NTP报文。之后，主动对等体向被动对等体发送时钟同步报文，报文中的Mode字段设置为1（主动对等体），被动对等体收到报文后自动工作在被动对等体模式，并发送应答报文，报文中的Mode字段设置为2（被动对等体）。经过报文的交互，对等体模式建立起来。主动对等体和被动对等体可以互相同步。如果双方的时钟都已经同步，则以层数小的时钟为准。
广播模式
在广播模式中，服务器端周期性地向广播地址255.255.255.255发送时钟同步报文，报文中的Mode字段设置为5（广播模式）。客户端侦听来自服务器的广播报文。当客户端接收到第一个广播报文后，客户端与服务器交互Mode字段为3（客户模式）和4（服务器模式）的NTP报文，以获得客户端与服务器间的网络延迟。之后，客户端就进入广播客户端模式，继续侦听广播报文的到来，根据到来的广播报文对系统时钟进行同步。
针对当前组网的特点，我们只需要分站的设备将NTP请求发往中心的某一私网地址即可，因此采用了以下命令：
//指定发送NTP报文的接口
ntp-service source-interface Ethernet0/1.1
//设定对等体模式下的目标地址与报文发出的源
ntp-service unicast-peer 10.61.3.26 source-interface Ethernet0/1
配置后，路由器每隔72秒钟会自动向指定的peer发送destination为10.61.3.26，source为Ethernet0/1接口地址的报文。
至此，通过NTP报文的触发，可以成功的触发建立指定源和目的的VPN SA，满足了用户的需求。
在我们庆贺大功告成之际，又一个问题提了出来，上面的两条命令能够自动触发建立IPSec SA，但是只能触发一对源和目的，而在实际使用中，用户存在着至少三对不同网段的互通需求，因此只触发一对网段是无法满足需求的。比如用户需要以下网段的VPN能够随时互访：
分站 中心
10.61.0.0 ------- 10.61.0.0
192.168.0.0 ----- 192.168.0.0
192.168.0.0 ----- 10.61.0.0
这样至少需要三对源报文进行触发。通过查看手册我们发现NTP可以同时配置不同的源和目的，配置命令如下：
ntp-service source-interface Vlan-interface100
ntp-service unicast-peer 10.61.3.26 source-interface Vlan-interface1
ntp-service unicast-peer 10.61.253.1 source-interface LoopBack0
ntp-service unicast-peer 192.168.61.1 source-interface Vlan-interface1
其中Vlan-interface1的地址属于10.61.0.0网段，LoopBack0的也地址属于10.61.0.0网段。
通过以上三条命令，实现了同时触发不同源和目的网段建立IPSec SA的需求。
通过debug ntp发现，NTP协议会周期性的轮训发送报文给不同的目的地，经过重新启动路由器测试，重启后中心依然可以主动访问分站的数据。
五、 总结：
它山之石，可以攻玉。