AR系列路由器传统VPN与DVPN的比较

岳斌 2007-03-15 发表

AR系列路由器传统VPN与DVPN的比较

1. 传统VPN存在的弊端

在现有的VPN组网方案中，三层VPN（Virtual Private Network）一般采用GRE或MPLS/BGP VPN两种方式。两种VPN虽然存在各自的优点，但是在实际的应用中都存在以下弊端：

（1）组网及配置复杂。三层VPN技术都采用的是点到点的隧道方案，当接入点数量为N，且需要建立一个全联通的VPN网络时，整个网络需要手工配置N×(N - 1) / 2个点到点的VPN隧道连接。

（2）可维护性及可扩展性差。对于一个已经组建好的VPN网络，若需要增加节点或修改某个节点的配置，那么其他所有节点都必须针对这个节点修改本地配置，维护成本较高。

（3）GRE 还存在无法穿透NAT网关的缺陷。GRE方式建立VPN隧道，如果出口有NAPT网关，那么就必须要一个公网地址直接对应一个内部地址来解决，需要大量的公网IP地址，这导致了GRE不能够应用于NAT网关内部。IPSec构建的VPN在原来的版本也是没有办法穿越NAT网关，目前通过将IPSec报文封装在UDP报文中进行发送，实现了NAT网关的穿越。

（4）GRE无法适用于动态IP的情况。GRE方式建立VPN隧道依赖于固定的IP地址，根本无法为拨号用户建立VPN。

（5）L2TP和GRE没有能够提供对传输的数据的加密保护，IPSec对通过IPSec VPN进行转发的数据提供了最安全的保护。

（6）IPSec在动态路由的支持存在一定的缺陷，IPSec的VPN隧道是基于数据流的，而不像GRE和L2TP基于接口建立VPN。在实现两个私有网络互联以后，两个私有网络之间没有办法实现路由的学习，这样给网络的动态规划带来了一定的问题。

2. DVPN的特点

DVPN不但继承了传统VPN的各种优点，更大程度上解决了传统VPN目前还没有解决的问题。配置简单、网络规划简单、功能强大，比传统的VPN更加符合目前以及未来的网络应用。其特点如下：

（1） 配置简单。一个DVPN接入设备可以通过一个Tunnel逻辑接口和多个DVPN接入设备建立会话通道，而不用为每一个通道配置一个逻辑的接口作为隧道的端点，大大的简化了配置的复杂度，提高了网络的可维护性和易扩充性。如果需要在已有的DVPN域中加入一个新的私有网络，只需要在DVPN的Client接入设备上配置需要加入的DVPN域的Server信息，新的DVPN Client就可以成功的添加到DVPN域中。

（2）自由穿越NAT网关技术。采用UDP方式的 DVPN。由于使用了UDP报文进行封装，可以自由穿越NAT网关。解决内网DVPN接入设备和公网DVPN接入设备之间的VPN连接，使NAT网关内部的私有网络和NAT网关外部的私有网络共同构建一个虚拟私有网络。

（3）支持依赖动态IP地址构建VPN。当在一个DVPN域内部构建隧道时，只需要指定相应的Server的IP地址，并不关心自己当前使用的IP地址是多少，更加适应如普通拨号、xDSL拨号等使用动态IP地址的组网应用。

（4）支持自动建立隧道技术。DVPN中的Server维护着一个DVPN域中所有接入设备的信息，DVPN域中的Client可以通过Server的重定向功能自动获得需要进行通信的其它Client的信息，并最终在两个Client之间自动建立会话隧道（Session）。作为Client的DVPN接入设备只需配置自己的相关信息和Server的信息，不需要知道其他Client的信息，极大地减少了网络的维护管理工作。

（5）注册过程加密技术。在Client向Server进行注册的过程中，需要先完成算法套件以及各种密钥地协商。使用协商出来的算法对注册过程中的关键信息（例如用户名、密码等）进行加密保护，还可以对注册的报文进行合法性检测，保证关键注册信息的安全性。

（6）身份认证技术。在Client向Server进行注册的过程中，Client可以根据配置需要对Server的身份使用pre-shared-key进行验证，保证Client接入一个合法的Server；同时Server可以根据需要使用AAA对需要接入到DVPN域的Client进行身份验证，保证只有通过身份验证的Client才可以接入到DVPN域。

（7）策略的统一管理技术。Client在Server端注册成功后，Server会将DVPN域中的策略发布给该Client。策略主要包括会话协商使用的算法套件、会话的keepalive时间、会话的空闲超时时间、IPSec使用的加密验证算法、IPSec SA的重协商时间等。在整个DVPN域中，所有的Session会使用相同的策略。

（8）会话协商过程中的加密技术。在Session协商过程中，所有的会话的控制报文都

会使用Server发布的算法套件进行IPSec加密保护。即在建立Session的会话协商过程中，根据Server发布数据的加密验证算法，为Session的数据通信协商IPSec SA。协商过程使用DH（Diffie-Hellman）进行SA的密钥协商。对于需要通过该Session进行转发的数据，如果需要加密处理，则通过IPSec使用Session协商出来的IPSec SA对报文进行加密处理后，通过DVPN进行转发，实现了转发数据报文的安全性。Session的IPSec SA支持重协商功能，可以根据需要指定进行IPSec SA重协商的时间，进一步保证数据的安全性。

（9）支持多个VPN域。DVPN允许用户在一台DVPN设备上支持多个VPN域。即一台路由器不仅可以属于VPN A，也可以属于VPN B；同一设备可以在VPN A中作为Client设备，同时还在VPN B中作为Server设备使用。在同一台DVPN设备上最多可以支持200个DVPN域，可以同时作为200个DVPN域的Server设备。这样大大提高了组网的灵活性，也可以更加充分的使用网络设备资源，减少了用户的投资。在实际的组网中为了保证各个DVPN域之间的隔离，如果在同一台DVPN设备上支持多个DVPN域，需要通过私网路由来实现不同DVPN域的隔离。

（10）动态路由的支持。DVPN可以对需要通过Tunnel接口发送的路由报文，通过所有的Session会话进行广播，从而实现整个DVPN域内的路由自动学习。实际应用中，DVPN配合动态路由协议，可以简化对需要接入到DVPN域的各个私有网络的规划，简化整个网络的配置，提高网络的维护性和自动化。