利用策略实现企业虚拟专用网（VPN）带宽监管Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/571/2021_2022__E5_88_A9_E7_94_A8_E7_AD_96_E7_c101_571861.htm VPN(虚拟专用网)是企业解决远程访问的首选。如下图，企业通过一个思科的VPN集中器，实现外网用户通过互联网访问企业内部的文件服务器等资源。不过企业配置了VPN虚拟专用网之后，也可能会带来一系列的问题。如当外部用户访问者比较多或者外部用户与文件服务器之间传输大容量文件时就会对企业内部用户正常访问互联网产生影响，因为其要占用比较大的带宽，无论是对防火墙还是企业内部的交换机或者路由器都会带来比较大的压力。而且如果对VPN的最大带宽进行限制，也可以把非法攻击者通过VPN对企业内部网络的攻击降低到最低。为此，对VPN虚拟专用网的传输带宽进行限制是有必要的。笔者在接下去的内容中就谈谈笔者是如何实现对这个VPN带宽的监管。 一、最高传输率限制的缺陷 现在市面上大部分的网络产品，都有最高数据传输率的限制。如在思科的VPN集中器中，为了满足用户对于VPN虚拟专用网带宽监管的需求，集中器就提供了最高的数据传输率。带宽监管功能可以设置隧道传输数据流的最高限制。如可以设置外部用户(全部)通过集中器访问企业内部文件服务器时最大的速率为 100Kbit/S(同时访问用户的流量总和)。集中器接收到的数据流，如果低于这个速率就传输.如果高于这个速率则就丢弃。 这个控制措施看起来是不错，但是，其有一个缺陷。众所周知，网络流量具有突发性的特点。如果规定的这么死的话，那么维护起来就会很麻烦。为此我们网络管理员往往希望

网络设备能够提供一些针对突发流量的应对措施。还好思科的VPN集中器没有让我们失望。在这个产品中，主要提供了两个指标让我们来监管VPN的带宽，这两个指标分别为监管速率和突发数据流的大小。监管速率就是我们常说的最高传输速率，专业的定义就是指稳定的隧道传输数据流的最高传输速率。突发数据流的大小是指在突发数据流被抑制到监管速率门限值以下之前，瞬时出现的突发数据流的最大值，也就是说其允许超过最大传输率的部分。集中器允许瞬时突发数据流的速率高于监管速率，达到突发速率。但是这有一个时间与量上的限制。如果一直有突发数据量且超过突发速率，则集中器就会认为这个数据流可能有问题，就会强制执行监管速率，集中器开始丢弃数据帧。 可见，监管速率(最大传输速率)与突发速率结合，可以实现对VPN带宽的灵活配置。二、针对不同的用户设置不同的传输带宽限制 由于不同的用户对于带宽的传输速率要求不同，为此网络管理员可以根据用户类型的不同来分别设置VPN带宽的限制。如对于普通用户来说，其由于只是正常的文件访问，故其基本上不会引起突发数据流(除非其帐户泄露，被别人用来攻击)，所以不需要为其设置突发速率，而只需要为其配置监管速率即可。而对于网络管理员来说，有时候出于文件服务器内核的升级(如文件服务器采用的是Unix系统)、服务器的调式等等的需要，可能会引发突发数据流。为此就可以为网络管理员同时设置监管速率与突发速率，以满足其突发数据流的需要。若要实现这个需求，则网络管理员可以通过组来实现。即可以为网络管理员设置一个维护组，然后设置监管速率与突发速率。然后把网络管理员加入到这个组中。而对于普通用户则可以

不设置突发速率，则其只能够大到最大的监管速率，即使有最大突发数据流的存在。 三、三步做好VPN带宽的监管设置 要对VPN带宽实现监管，主要通过三个步骤来实现，分别为定义监管策略、降策略分配到特定的接口、分配组等。具体的配置如下： 第一步：配置监管策略 网络管理员若要配置VPN集中器的监管策略(以思科VPN3000为例)，主要是在Bandwidth Policies窗口中实现。在这个窗口中主要分为上下两个部分。上面部分主要用来配置预留带宽，下面一部分就是用来配置监管速率策略。在配置监管速率策略的时候，主要就是配置两个值分别为监管速率(PoliclingRate)与正常突发数据流大小(NormalBurstSize)。注意这个监管速率不同的产品其最大的允许的速率是不同的。故管理员在配置之前需要先查看相关的说明书，然后再进行配置。以VPN3000为例，其监管速率的范围为 56-100Kbit/s。默认情况下为56Kbit/s。在配置监管速率与正常突发数据流大小这两个参数时，笔者有如下建议两个建议。 一是注意集中器传输移动速率低于监管速率的数据流，集中器将会丢失数据帧。为此到底多大的监管速率是合适的，网络管理员还是需要根据企业自身的需求来定。笔者的做法是，刚开始不启用配置监管策略。对VPN的网络流量先规测一段时间，得出一个合理的值。经过一个月的规测之后，再起用监管策略。如此的话，网络管理员就可以有参考的依据。从而就不会因为这个监管速率配置不合适而给用户的正常访问带来不利的影响。 二是确定了合适的监管速率之后，是否要启用突发速率要结合企业的实际情况来定义。如果企业的网络应用中，有些会触发突发数据流，则就需要启用。否则的话，就没有启用的必要。因为这个突发

数据流很有可能是病毒或者木马之类造成的。所以不启用这个突发数据流也是对企业内部网络的一种保障。根据笔者的经验，笔者建议对于普通用户来说，可以不设置正常突发数据流大小。而对于管理员来说，出于日常维护的需要，就可能需要设置这个正常突发数据流大小，以满足其维护过程中出现的突发数据流。如现在笔者配置了一个监管策略，监管速率与正常突发数据流大小都采用默认值。那么任何一个分配了这项策略的远程用户，他的稳定隧道传输数据流的最高速率为56Kbit/s。集中器在通过丢弃数据报限制数据流之前，他可以支持的瞬时突发数据流为10500字节(正常突发数据流的默认大小)。网络管理员可以根据企业的实际应用来调整这两个参数。 第二步：将策略分配给集中器接口 策略配置好之后，跟访问控制列表一样，其默认情况下是不会启用的。网络管理员需要把这个策略分配给集中器的接口之后才会启用。要为某个特定的接口启用监管策略，则需要打开接口配置窗口，如Ethernet2窗口。在这个窗口中，可以设置这个接口是否需要启用带宽管理。如需要启用的话，则就可以在此为接口分配其要使用的策略。网络管理员可以在带宽策略(Bandwidth Policy)处选择刚才建立的监管策略。 在监管策略应用时，笔者还需要向网络管理员提醒一点，即连接速率对监管策略应用的影响。链接速率必须是基于可用的因特网带宽而不是Lan物理连接速率。如果链接速率低于监管速率的综合，则部分远程用户建达不到监管速率。这是什么意思呢?简单的将就是当互联网传输速率比监管策略设置的监管速率要低的话，则远程用户就永远达不到监管策略规定的最大传输速率。 第三步：分配组 思科的集中器中，即可以将策略应

用到用户，也可以将策略应用的组中。如果企业需要远程访问的用户比较多的话，而且有需要为其分配不同的监管策略，则最好能够通过组来管理，以减少维护的工作量。其实这个步骤跟上面第二个步骤是并行的，在同一个配置窗口中实现。在配置的时候，网络管理员需要注意 VPN集中器的一个默认法则。即如果网络管理员没有为远程用户所在的组设置专门定义的监管速率，则VPN集中器会将接口的监管速率直接分配给用户。也就是说，VPN集中器不像微软操作系统，默认情况下其是不通过组来管理用户的。这一点网络管理员要特别注意。 