思科:VPN硬件客户端与软件客户端优劣分析Cisco认证考试
 部属完成思科的VPN集中器后接下去网络管理员需要考虑的内容是为远程客户选择一个合适的VPN客户端。远程接入客户端依赖VPN客户端来建立并维持与VPN集中器之间的连接。现在思科推出的 客户端主要有两种，分别为基于软件的客户端和基于硬件客户端。作为网络管理员，有必要了解这两种客户端的优缺点，并根据企业的实际应用情况在部属VPN应用时为用户选择合适的客户端。 一、软件客户端分析 思科的VPN客户端在购买集中器的时候是与此一起交付的。它跟硬件客户端相比最突出的优势就在于软件客户端往往没有许可证的限制。注意这是指思科的软件客户端。思科的软件客户端可以运行在多个系统平台上，如微软的操作系统或者Linux操作系统上。也就是说，它是跨平台的。下面笔者以微软的 VPN客户端平台为例，谈谈它的特点。 思科VPN客户端与其他软件客户端相比，最突出的特色就在于客户端支持防火墙功能。这主要是为了通过提高VPN客户端的安全性来保障VPN连接的安全。基于微软客户端的防火墙主要有三种模式。一是AYT模式，它表示是否需要防火墙是可选的。在客户端连接VPN集中器之前，网络管理员出于安全方面的考虑，可能会要求远程电脑使用防火墙。AYT的功能主要就是验证远程客户端中是否存在防火墙，无论有否客户端软件都会把这个信息反馈给集中器。然后根据集中器设置的安全规则，来判断是否允许这个用户建立VPN连接。 第二种是状态防火墙。他表示防火墙永远开启

。状态防火墙模块只能由远程客户端启动或者关闭。在状态防火墙模式下，防火墙会使用一种缺省的策略。即将阻止所有与出向会话无关的来回会话。一旦用户启动防火墙，他将一直处于开启状态，即使关闭VPN隧道也是如此。可见这个模式下对于安全要求比较高。 第三种模式是集中策略保护模式。在这种模式下，是否允许远程客户端的流量通过VPN集中器，主要要根据网络管理员设置的规则来判断。在远程用户建立连接之后，集中器会将网络管理员预先定义的访问策略传输给软件客户端。然后VPN客户端再将这个策略转交给客户机上的防火墙。防火墙就会根据定义的策略来判断是否允许数据流通过。可见，集中策略模式在保障VPN连接安全的同时，也给了网络管理员一个灵活的管理平台。 二、硬件客户端分析 网络管理员除了可以使用软件客户端外，还可以通过硬件客户端来达到VPN连接的需求。如果采用硬件客户端的话，网络管理员可以直接把远程站点的 PC插入硬件客户端，而不必在远程站点的PC上加载VPN客户端或者额外的应用。因为在思科提供的硬件客户端内本身就带有VPN软件客户端。这个硬件客户端就好像是一台PC，他直接与VPN集中器相连，建立VPN隧道。然后远程用户就可以通过硬件客户端使用这个VPN隧道。 到目前为止，思科提供的硬件客户端包括两个版本，分别为3002版本与3002-8E版本。这两个版本主要的不同在于接口。3002版本中只包含一个专用接口与一个公用接口。而在3002-8E版本中，则提供了一个公用接口、八个专用接口与AUTOMDIS接口。专用接口是一个内置的八端口，通常情况下这个专用接口时被锁住的，而且无法进行配置。而AUTOMDIS接口可以方便网络管理员的管理，因为

有了它的存在，网络管理员可以避免使用交叉线。另外如果网络管理员采用硬件客户端的话，则需要对其进行配置。为了VPN连接的安全，在对VPN硬件客户端进行配置的时候，最好可以利用IPSec加密技术或者安全外壳(SSH，而不是安全性相对较差的Telnet)来管理配置。 三、硬件客户端与软件客户端的选择 无论是硬件客户端还是软件客户端，都可以帮助用户建立与VPN集中器的连接。那么网络管理员怎么知道哪个客户端好一点呢?其实两个客户端各有千秋，如果要说那个好，笔者也说不上来。笔者认为这两个客户端没有好坏之分。只有结合企业的实际应用场景，才能够判断出哪种类型的客户端更加适合企业。 那么网络管理员在做出选择的时候，该从哪几个方面入手呢?笔者认为，管理员出要从几下几个方面出发，判断到底哪个更加适合企业。 一是从远程用户的移动性考虑。如果远程用户的位置是经常移动的，如一些出差的员工他们需要远程访问时位置并不固定。有时候可能是在网吧，有时候又在宾馆。在这种情况下，往往还是采用软件客户端好。如果采用硬件客户端的话，难道还让员工背着个硬件满世界跑?这显然不现实。而且到出差的员工比较多，则网络管理员还要给他们每人配一个硬件客户端?这企业不是当了冤大头了吗。反之，如果远程访问用户的位置比较固定，如是通过异地办事机构连入VPN等等。此时，采用硬件客户端可能比较有利。 二是要考虑远程用户的数量。如果采用软件客户端的话，VPN对于远程用户来说就不是透明的。这会增加网络管理员工作的压力。若采用软件客户端的话，如果用户要连接VPN，网络管理员必须在每个需要远程访问的用户PC上安装VPN客户端软件。而远程用户每次在需要远程访

问时必须要手工启动软件客户端，并输入访问帐户与密码。另外网络管理员还需要负责客户端的日常维护与版本更新。对每个单独的软件客户端进行这些维护工作量将会很大。随着用户的增加这个工作会成倍增加。故所有的这些都会增加网络管理员的工作量。但是硬件客户端比软件客户端来说，有一个很优越的地方，就是硬件客户端对于远程用户来说是透明的。即远程用户需要建立VPN连接时，不需要专门去启动VPN客户端软件。因为这个连接硬件客户端已经帮助远程用户完成了。而且采用硬件客户端的话，其数据的处理效率更高。远程用户可以利用现成的连接来进行远程访问。而且网络管理员不用维护员工电脑上的软件客户端。故当用户比较多时硬件客户端可能更加有吸引力。虽然软件客户端没有许可证的限制，但是当用户比较多时，这个相比其维护的工作量来说，反而是小儿科了。不过，笔者觉得这仍然受到远程用户移动性的限制。也就是说，如果企业的远程访问用户再多，如果位置都是移动的，那么也只能够使用软件客户端，而不适合采用硬件客户端。也就是说，员工数量这个判断条件，是以用户的移动性条件为前提的。 笔者现在采用的客户端是硬件客户端与软件客户端结合的方式。如笔者企业现在全球都有分支机构与办事处。他们平时都需要通过VPN连接到企业总部的网络。为此，笔者对于这些有固定位置的分支机构或者办事处，就让他们通过硬件客户端来接入到企业的内部网络。由于部署了硬件客户端，笔者就一一维护这些员工PC的软件客户端。而只需要维护他们的一台硬件客户端即可。这可以大大的减少笔者的工作量。同时硬件客户端相对软件客户端来说，具有更高的安全性。 而对于平时需要出

差的一些员工，他们需要远程访问的需求时，则是通过软件客户端来实现的。因为他们的位置不固定，而且也不可能给他们一台硬件客户端让他们带着满世界跑，所以他们主要是通过采用VPN软件客户端来进行远程访问。笔者企业需要出差的员工比较多，再加上有些员工需要在家里办公也要进行VPN远程连接，笔者粗略统计了一下有差不多100人左右需要这个VPN远程访问的需求。还好他们大部分时间都是错开访问，故并不会对VPN集中器造成太大的压力。而且VPN软件客户端是不用另外购买的，是跟着VPN集中器一起交付的.同时其又没有许可证的限制。所以在软件客户端上的投资，基本上不用。除了要付出一点时间维护这些客户端。 故对于是否是采用软件客户端还是硬件客户端，笔者的建议是根据远程用户的移动性与用户数量来考虑。如果远程用户在进行VPN连接时都没有固定的场所，那么最好采用软件客户端。如果远程用户有固定的位置办公，同时远程访问用户的数量又比较多，那么最好采用硬件客户端。虽然硬件客户端的初始投资要大一点，但是长久以往这个投资还是值得的。 