思科认证:企业数据加密需选择合适的地方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__E6_80_9D_E7_A7_91_E8_AE_A4_E8_c101_571876.htm 给数据加密是网络管理员常用的提高网络数据传输安全的措施之一。但是，网络管理员需要注意的是，给数据加密后再传输，会额外的增加网络设备CPU 的压力，会明显降低数据的传输速度。如接收到加密后的思科路由器，必须要先读取数据包包头的一些信息，然后才能够确定转发的目的地。这也就是说接收路由器要先对加密后的数据包进行解密。然后读取相关信息后再对数据进行加密处理后再转发出去。故这个解密、加密的处理过程就会大大增加网络设备数据转发的压力。 在使用思科的交换机或者路由器对数据进行加密时，网络管理员可以选择在应用层、网络层或者数据链路层等多个地方部署加密策略。但是，每个不同的地方部署加密策略，其对路由器等网络设备的影响是不同的。也就是说，采取不同的加密策略，路由器的开销是不同的。故网络管理员需要了解不同加密策略下路由器等网络设备的开销问题，然后根据企业的实际情况选择合适的加密策略。如此才能够实现安全与数据传输两不误。 一、在应用层实现加密 网络管理员可以在应用层上实现对数据的加密。如现在比较流行的HTTPS协议，就是在应用层层面上实现加密的一个典型代表。HTTPS协议以保密为目标研发的一种技术。简单的说他就是HTTP协议的安全版，他是在SSL协议上实现的一种加密手段。它使用了HTTP协议，但是他们之间有一个很大的不同，即HTTPS协议存在不同于HTTP的默认端口及一个加密身份验证层。这个安全协议的

最初研发由网景公司进行，提供了身份验证与加密通讯方法，现在它被广泛用于互联网上安全敏感的通讯。如现在不少网络设备可以通过浏览器来进行管理。为了提高设备的安全性，通过浏览器管理网络设备的话，都是采用安全的HTTPS协议，而不是HTTP协议。为此如故应用程序有一个WEB接口或者一个后断服务器，对于这种情况出于安全方面的考虑，最好的选择就是通过安全的超文本协议和安全套接字层来(HTTPS)加强WEB浏览器和数据服务器之间传输数据的安全性。 可见，现在支持应用层加密的协议也是比较多的。这主要是因为在应用层进行数据加密的话，有一个非常明显的优点，几可以按照不同的需要有选择的对数据进行加密。如现在网络管理员需要远程维护一台网络设备。现在这个管理员有三个不同的选择，他可以分别通过浏览器、SSH、Telnet这三种方式来实现远程管理。而如果在应用层实现加密的话，那么管理员就可以选择对于那种方式进行加密。如管理员可能认为通过浏览器管理网络设备安全风险比较大，那么可以为浏览器这种方式设置应用层加密手段，来提高网络设备的安全性。但是管理员会认为采用Telnet远程管理路由器比较安全，不需要采用加密措施。那么通过 Tennet传输的数据就不会加密。故如果在应用层实现数据加密，其用户的选择性会比较强一点。可以根据不同的应用来选择是否需要加密。由于不需要多所有的数据都采取加密处理，故中间的网络设备其开销也会少的多。 不过这也有一定的缺陷。这个缺陷主要体现在两个方面。一是要委托用户控制。也就是说，是否要采取加密措施，其主动权很大一部分在用户手中。由于用户缺乏安全意识等原因，这会降低加密措施所带来的安全性

保障。二是增加了在每个服务器上配置加密措施的工作量。而且由于每个服务器上都要进行单独的培植，这不利于在企业内部实现一致的安全策略。所以，在应用层面采取加密，虽然可以降低中间网络设备的开销，但是增加了网络管理员的工作量。 二、在网络层上实现加密 网络管理员也可以选择在网络层上实现加密，这也是现在最流行的一种加密措施。在网络层实现加密的话，就不用考虑应用层的管理软件了。也就是说，为了加密网络通信流，不许要更新任何主机上的应用。即使应用软件不支持加密功能，则只要在网络层上对数据进行加密，则应用层的数据在网络上传输也是加密的。因为应用层的数据先要发给网络层，然后有网络层对数据进行加密。 现在网络层加密技术最火的就是IPSec技术了。IPsec在网络层提供安全服务，它使系统能按需选择安全协议，决定服务所使用的算法及放置需求服务所需密钥到相应位置。IPsec 用来保护一条或多条主机与主机间、安全网关与安全网关间、安全网关与主机间的路径。IPsec 能提供的安全服务集包括访问控制、无连接的完整性、数据源认证、拒绝重发包(部分序列完整性形式)、保密性和有限传输流保密性。简单的说，IPSec主要实现两个功能，一是对数据进行签名，防止被修改.二是对数据进行加密，防止被窃听。而对数据进行加密，就是实现在网络层上的。 网络管理员若在网络层实现对数据的加密，其优势有很多。 一是提高网络设备的性能。数据从应用层传输到网络层，每过一个层都会在上一层数据的基础上添加一写包头信息，如所采用的端口等等。如果在网络层上实现数据加密，第三层和第四层的有些信息是不会被加密的。这些不加密的信息主要就是网络设备用来选择路

由用的。也就是说，使用网络层加密的话，网络管理员可以在网络上任何点实施加密。因为数据首部关键信息(如端口或者协议信息)没有被加密，而只是数据包的内容被加密。那么加密过的数据包像任何其他数据包那样可以在网络中正常传输。所以加密必要的信息，不加密这些用来选路由的信息，即可以提高数据的安全性，同时也不会造成网络设备过多的开销。 二是不依赖与网络所实现的拓扑类型。在网络层中采取加密，由于不加密重要的包头信息，故其可以跟网络的拓扑类型无关。如IP安全策略，其可以在任何的网络拓扑中使用。股网络管理员如果在网络层中实现加密的话，则就不用考虑网络拓扑问题。 三是得到思科IOS软件的支持。现在互联网中应用的最多的网络设备就是思科的网络设备。而且说实话，其他网络设备厂商也都把思科当作老大哥。所以现在主流的网络设备基本上都支持在网络曾上的加密技术。故像IPSec等网络层加密技术，兼容性是比较高的。 四是不要求中间的路由器或者网络上的其他网络设备提供支持。网络层的数据加密与解密主要是在对等路由器上实现的。跟对等路由器中间的网络设备是无关的。所以，其不需要中间网络设备的支持。 但是，网络层加密技术也存在一个问题。他可能会跟其他的一些网络技术产生冲突。如采用了IPSec网络层加密技术之后，就很难跨越NAT服务器。因为NAT服务器需要修改数据包的包头信息，而IPSec网络层加密技术则是不允许的。如果一定要实现的话，只能够通过UDP封装等等。 三、在链路层上实现加密 网络管理员也可以在数据链路层上实现加密。不过笔者是不建议采用这种加密方式。数据链路层加密是在路由器以下的设备上执行的。由于在数据链路层加密

中，网络层首部以及协议类型、端口信息等都被加密。这会给路由器等网络设备在转发数据时造成不必要的麻烦。 在链路层上实现加密确实也能够为网上传输的数据提供安全保证。所有消息在被传输之前进行加密, 在每一个节点对接收到的消息进行解密, 然后先使用下一个链路的密钥对消息进行加密, 再进行传输。可以网络管理员需要注意的是，在到达目的地之前, 一条消息可能要经过许多通信链路的传输。而由于包括路由信息在内的链路上的所有数据均以密文形式出现，链路层加密就加密了被传输消息的源点与终点，故在每一个中间传输节点消息均要被解密后重新进行加密(数据包转发的需要)。故中间设备的开销就会比较大。另外，链路加密通常用在点对点的同步或异步线路上,。这就要求先对在链路两端的加密设备进行同步, 然后使用一种链模式对链路上传输的数据进行加密。这就给网络的性能和可管理性带来了副作用。 所以说在链路层实现数据加密的话，其副作用是比较大的。笔者现在在网络设计与部署中，从来不在链路层上实现加密。可见，在数据加密位置的选择上，链路层加密基本上可以不考虑。网络管理员现在只需要根据自己企业的实际情况，在应用层与网络层加密之间作一个分析比较，选择一个合适的位置即可。 