思科认证:利用SSL保障企业网络运输稳定与安全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_ti2020/582/2021_2022__E6_80_9D_E7_A7_91_E8_AE_A4_E8_c101_582068.htm 众所周知，不同主机之间的网络数据传输主要是通过TCP/IP网络协议来完成的。无论是企业局域网数据传输，还是互联网上的数据传输，都是如此。但是，令人想不通的是，在当初TCP/IP协议的设计过程中，并没有提供任何安全性。也就是说，光凭TCP/IP协议，并不能过保障数据在网络中的安全与稳定的传输。为此，数据在网络中的安全性要依赖于高层的应用程序。互联网技术发展到现在，已经有不少提高网络运输稳定与安全的解决方案。笔者今天结合Cisco技术谈谈如何通过SSL来实现这个需求。 SSL中文名字叫做安全套接层协议，他使用TCP/IP为高层协议建立安全连接。它运行在TCP/IP和高层协议之上，提供数据传输的安全性。SSL协议其包括两个分支，分别为SSL纪录协议与SSL握手协议。 一、三步完成SSL纪录协议 SSL纪录协议相对来说，比较简单。它定义了数据在网络中传输的格式，并对此采取加密处理。同时还提供了一些验证手段，防止在传输过程中数据被人为的破坏，从而影响数据传输的稳定性。要实现这些目的，只需要简单的三步即可。 第一步：分块。当上层的数据被转移到SSL协议所在的层之后，数据将会被分块。从上层传递下来的数据往往是以明文形式传送的。通常情况下，分块过后的数据不会超过214字节。分块的时候，一般不会考虑数据的内容形式，而只考虑大小。即具有同样类型的不同纪录消息会被组合为一个纪录.而如果一个纪录容量比较大的话，也会被分割为多个块。

第二步：压缩并加密。分块之后，SSL协议就会对要传输的数据使用压缩算法进行压缩，并且在压缩过程中同时进行加密处理。压缩算法必须保证数据在压缩后不会被丢失。当另外一端接收到数据之后，就会采用对应的解压算法对数据进行解压缩，同时完成数据的解密过程。 第三步：纪录有效载荷的保护。在数据传输过程中，另外一个需要关注的问题，就是传输数据的稳定性。也就是说，传输的数据有没有被意外的更改等等。SSL协议也提供这方面的保护。当完成对数据压缩与加密之后，SSL纪录协议会计算出完整的校验值，也就是所谓的消息鉴别码。在传输数据的时候，这个消息鉴别码会随同上面的块一同被加密传送。在接收端，数据被解密、解压缩.然后也会重新计算着消息鉴别码，以验证数据是否在传输过程中被意外修改。 二、SSL握手协议 SSL纪录协议只是在单机上对信息进行重新分块并进行压缩与加密，而没有涉及到网络连接。SSL握手协议则主要用来解决主机之间的连接问题。SSL握手协议使用SSL纪录协议，在两台支持SSL的设备之间通过交换一系列信息，以建立SSL连接。SSL握手协议在建立连接的过程中，主要完成对服务器与客户之间的相互鉴别、确定所要采用的加密算法、通过使用公开密钥加密技术产生共享的加密信息、建立加密的SSL连接等等。 建立一个SSL会话要比SSL纪录协议复杂的多，往往需要通过多个步骤才能够完成。这里出于篇幅的限制，也就不再展开了。大家若有需要可以去参考相关的书籍。笔者这里主要对几个容易搞混的地方做一些说明，以便于大家应用SSL协议。 一是加密方法的选择。在SSL建立会话传递数据的过程中，要确保其路过的每一个网络设备都支持SSL协议。否则的话，就会出现数据

传输上的问题。而现在包括思科在内的网络设备，大部分已经都支持SSL协议。但是，SSL协议所采用的加密方法有上十种。虽然现在的网络设备基本都支持SSL协议，可是不一定会支持所有的加密算法。为此，SSL协议会在建立会话的过程中，选择大家都支持的一种加密算法。在对于一些安全性级别要求比较高的场合中，网络管理员要对其具体采用的加密算法进行监控。若无法满足企业的安全性需求，则要及时的更换设备或者对设备进行升级，以满足比较高的加密算法以及安全性需求。 二是要注意加密并不等于不能够破解。SSL的连接是加密的。在客户机、服务器之间的所有传送数据通过SSL协议处理之后，都是加密的，这为数据传输提供了很高的机密性。SSL协议在确定了所使用的加密算法之后，一个初始化的握手过程会产生密钥，加密算法就会采用这个密钥。但是，要值得注意的就是，并不是说加密之后的数据就不能够被破解。而只是说，增加了这个破译的难度。而这个难度系数到底达到多少，又是由这个加密算法说决定的。虽然说在SSL会话过程中，SSL协议会自主选择一个大家都支持的加密算法。 但是，出于某些特殊性安全的需要，有时候网络管理员要对这个进行干预。如网络管理员可以禁用某些网络设备上的级别低的加密方法。从而在数据传输中，要么不传，要传就要用一些高级加密方法处理。这虽然不利于网络传输的稳定性，但是可以满足一些对于数据安全有特殊需要的客户。 三是可以通过配置SSL协议为其他不安全的服务提供身份验证等功能。如在实际工作中，采用Telnet协议远程管理服务器或者网络设备，不怎么安全。这主要是因为Telnet协议在数据传输过程中，无论是用户名口令，还是执行命令，都是

明文传输的。很显然，这会给入侵者一个可乘之机。另外，诸如TFTP(简单文本传输协议)也是不安全的，因为其没有提供身份验证机制。在这种情况下，网络管理员就可以把SSL协议与这些不安全的协议结合起来，在享受它们便利的同时，又保障他们的安全性。 另外，IPSec技术也可以起到类似的作用。简单的原理就是把路由器等关键设备当作服务器，而把用户的主机当作客户端。在服务期上可以设置安全策略，必须要采用加密技术。如此的话，在客户端跟服务器端进行协商的时候，服务起就会告诉客户端，你如果想跟我通信，必须要采用我指定的加密技术，否则的话，休想跟我通话。通过这种措施，就可以在客户机与服务器之间强制建立起一个安全通道。 如此，即使HTTP等协议采用明文形式传输数据，也不用担心。因为虽然HTTP协议没有采取安全策略，但是当HTTP报文在网络中传输的时候，诸如SSL或者Ipsec等安全技术为其保驾护航，通过加密等技术保障其传输过程中的安全性。 四是在VPN技术上与SSL协议集成，提高远程访问的安全性。虽然传统的VPN技术也提供了一些安全身份认证机制，但是普遍认为其自带的安全解决方案是不安全的。传统的VPN技术下，黑客入侵、身份欺诈等攻击行为时有发生，而且得逞的案例也不在少数。而如果在VPN技术上实现SSL协议，则其远程访问的安全性会发生根本的改变。也许会有人说，采用IPSec技术同样可以取得类似的效果。 确实如此，但是如果企业采用IPSec技术来保障VPN安全的话，则必须要满足一个前提条件，即企业的网络架构不能够经常变化。也就是说，IPSec技术确实在安全性方面具有杰出的表现，但是其灵活性就不如SSL那么高了。若企业的网络还是处于变革中，

那么笔者建议网络管理员还是利用SSL协议来武装VPN，来实现一个相对安全的远程访问。 五是在WEB服务上集成SSL协议，以实现安全性。我们都知道，WEB服务一向被认为是一种不安全的网络访问行为。但是，若果在WEB服务器上能够实现SSL协议，那么，其就可以变得很安全。如现在有不少的电子商务网站，其在访问时需要使用HTTPS来进行访问，而不是传统的HTTP。他们就是采用了SSL协议。 如果需要WEB服务器支持SSL通信，就必须要为WEB服务器设置SSL证书。如在微软的服务器架构中，WEB服务器可以向证书颁发机构申请证书。安装证书之后，网络管理员就可以通过Internet服务管理器，将WEB服务器下面的虚拟目录配置为要求采用SSL访问。注意，此时可以制定一些特定的文件、目录或者虚拟目录采用SSL协议，而不需要所有的目录。如此配置后，当客户要访问这些WEB服务器中的内容时，服务器就会告诉用户要利用SSL协议进行通信。如果客户的主机不支持SSL协议(如已经被认为的禁用掉)，则服务器会拒绝与其进行通信。从而爆炸功能WEB服务器资源的安全性。 