



SUNDRAY
信锐技术

数字证书及CA的解读

2017 年 9 月 14 日

大家都知道,不同场景安全要求不一致,企业wifi接入需要满足不同场景的灵活认证方式,信锐无线控制器拥有多重接入认证方式,其中对员工的认证方式有:802.1x、CA证书、Portal、WAPI、MAC地址。那么,什么是数字证书以及CA呢?

● 什么是数字证书?

“数字证书”洋文也叫“digital certificate”或“public key certificate”

数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。通俗地说,证书就好比公章,通过公章,可以证明一封信件确实是对应的公司发出的。

● 什么是CA证书?

CA证书,顾名思义,就是CA颁发的证书。CA机构称证书授权中心(Certificate Authority)

CA数字证书就是互联网通讯中标志通讯各方身份信息的一系列数据,提供了一种在Internet上验证您身份的方式,其作用类似于司机的驾驶执照或日常生活中的身份证。

信锐NAC内置CA证书颁发中心,并支持CA证书自动更新,无需另外部署一台证书服务器,简化证书认证结构,实现安全的“实名制”,不必购买单独的CA认证体系,为企业减少了投入成本。

● 什么是证书之间的信任关系?

用一个证书来证明另一个证书是真实可信。通俗地说,公章A信任公章B,用公章B也可以达到证明一封信件是A公司发出的。

● 什么是证书信任链?

实际上,证书之间的信任关系,是可以嵌套的。比如,C信任A1,A1信任A2,A2信任A3.....这个叫做证书的信任链。只要你信任链上的头一个证书,那后续的证书,都是可以信任。

● 什么是根证书?

“根证书”的洋文叫“root certificate”,根证书是整个证书体系安全的根本。所以,如果某个证书体系中,根证书出了问题(不再可信了),那么所有被根证书所信任的其它证书,也就不再可信了。

● 数字证书有啥用?

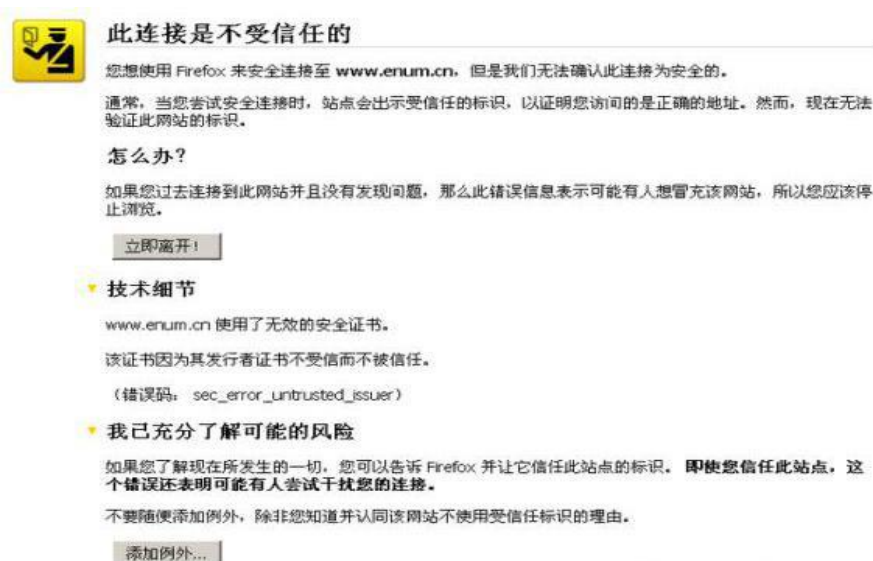
1) 验证网站是否可信(针对HTTPS)

通常,我们如果访问某些敏感的网页(比如用户登录的页面),其协议都会使用HTTPS而不是HTTP。因为HTTP协议是明文的,一旦有坏人在偷窥你的网络通讯,就可以看到网络通讯的内容(比如你的密码、银行帐号、等);而HTTPS是加密的协议,

可以保证你的传输过程中，坏蛋无法偷窥。

但是，千万不要以为，HTTPS 协议有了加密，就可高枕无忧了。HTTPS 协议除了有加密的机制，还有一套证书的机制。通过证书来确保，某个站点确实就是某个站点。

有了证书之后，当你的浏览器在访问某个 HTTPS 网站时，会验证该站点上的 CA 证书。如果浏览器发现该证书没有问题（证书被某个根证书信任、证书上绑定的域名和该网站的域名一致、证书没有过期），那么页面就直接打开；否则的话，浏览器会给出一个警告，告诉网站证书有问题。



2) 验证某文件是否可信（是否被篡改）

证书除了可以用来验证某个网站，还可以用来验证某个文件是否被篡改。当查看该文件的属性，会看到如下的界面，会注意到到上面有个“数字签名”的标签页。如果没有出现这个标签页，就说明该文件没有附带数字签名。（如ownCloud的安装文件）

