使用 Windows Server 2016操作系统自签名CA证书服务器（Microsoft Active Directory 证书服务） 实现SSL VPN证书双向认证

SSL PKI SSL VPN IKE **胡伟** 2020-12-14 发表

组网及说明

关于CA证书服务器的安装，请参考如下知了链接：
https://zhiliao.h3c.com/Theme/details/136608

SSL VPN证书认证需要防火墙和客户端同属于一个CA证书服务器下。
该认证的过程如下：
(1) SSL VPN用户选择自己的SSL VPN用户证书（客户端证书），用户设备会将该证书发送给SSL VPN网关；
(2) SSL VPN网关用CA证书检查SSL VPN用户证书是否可信：如果可信，则继续进行下一步；如果不可信，则不能建立SSL连接；
(3) SSL VPN网关从SSL VPN用户证书中的CN字段提取用户名，并将该用户名提交给AAA模块进行授权和计费。
(4) 如果有证书和密码的组合验证，在步骤（3）下还需要 SSL VPN网关从SSL VPN用户证书中提取用户名与输入的用户名进行比较。

- 若一致，则网关将用户名和密码提交给AAA模块进行认证、授权和计费；
- 若不一致，则认证不通过。

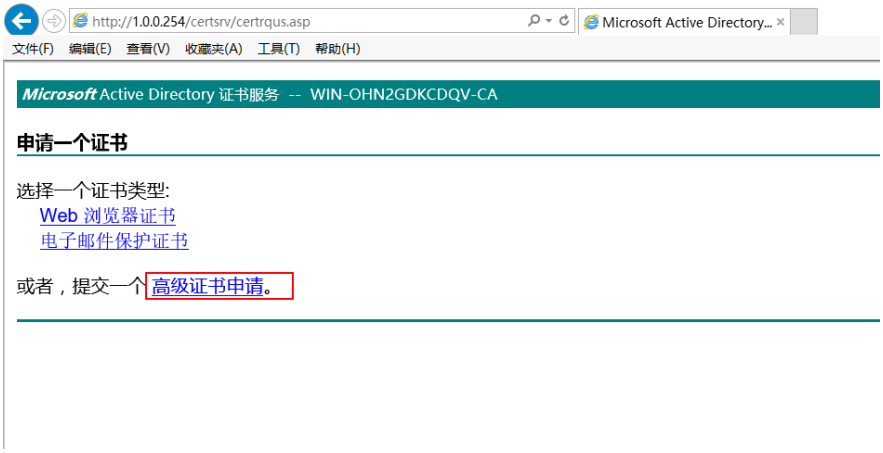
说明

· 证书认证本地设备中必须存在该用户。
· SSL VPN客户端证书中的CN字段必须和该SSL VPN用户的用户名一致。

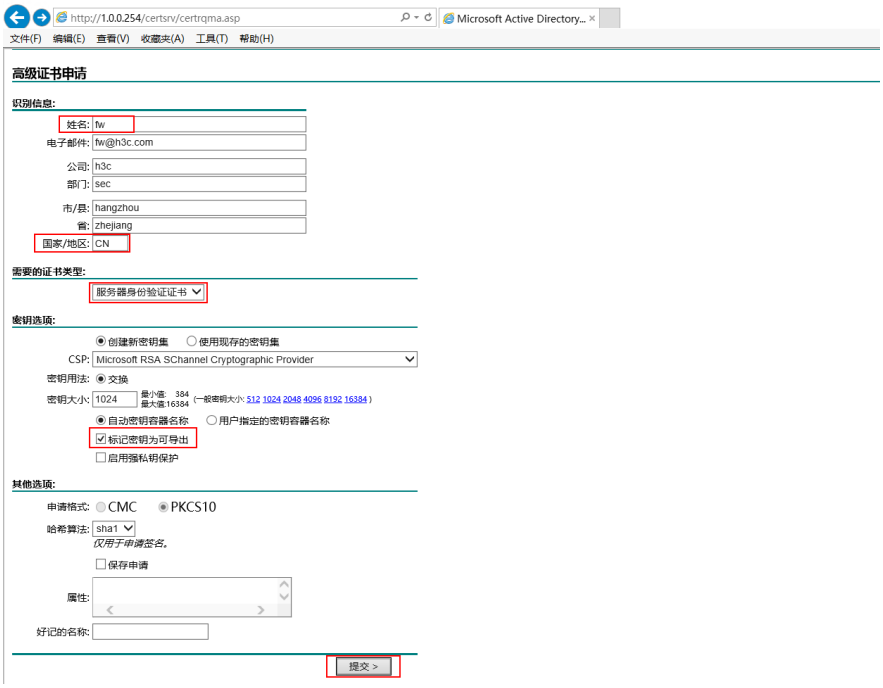
配置步骤

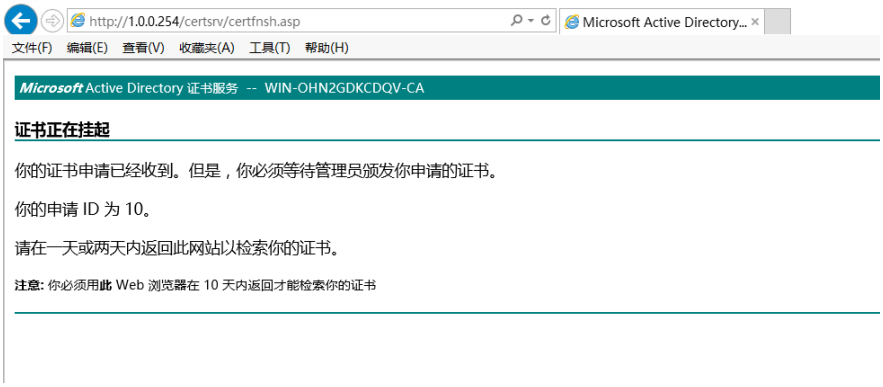
配置步骤主要分为以下三个方面：
（一），向CA服务器申请服务器证书、客户端证书以及CA证书。
（二），安装客户端证书。
（三），防火墙PKI引入CA证书和服务器证书。
（四），SSL VPN网关引用关联对应PKI的SSL服务器策略。
（五），拨测验证。

1， 向CA服务器提交SSL VPN服务器证书、客户端证书申请。输入Microsoft Active Directory 证书服务链接，如：http://1.0.0.254/certsrv/，按照以下步骤进行。

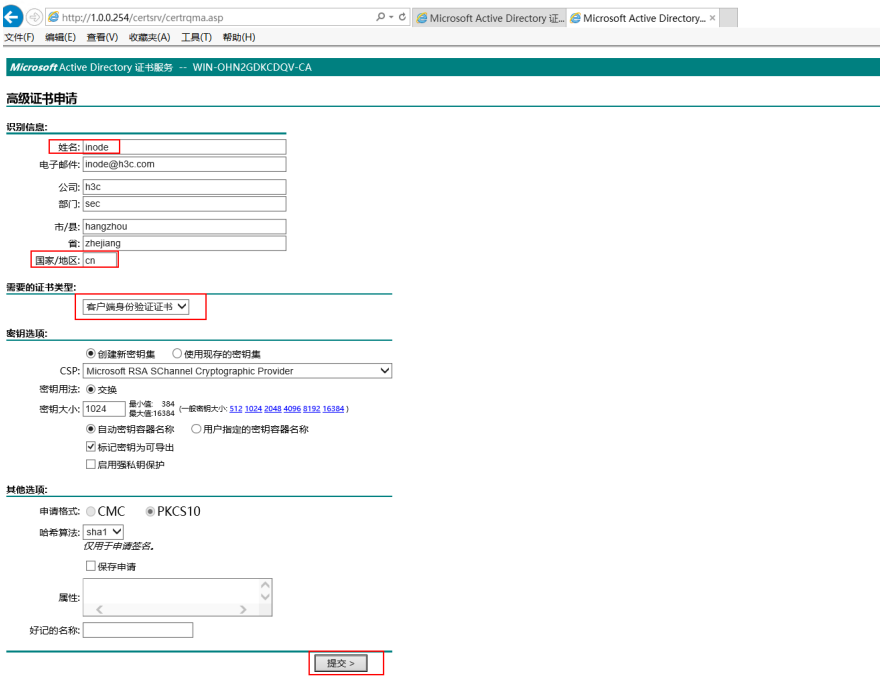


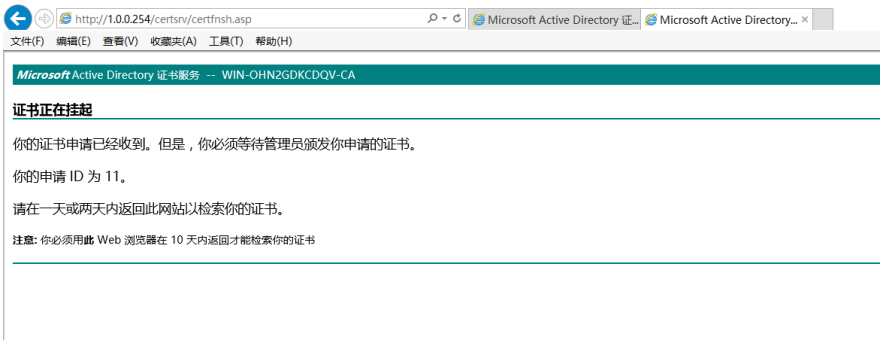
2、这里申请SSL VPN服务器证书即防火墙本地（local）证书，**姓名(Common-Name)**设置为**fw**，证书类型为**服务器身份验证证书**，并**标记密钥为可导出。**



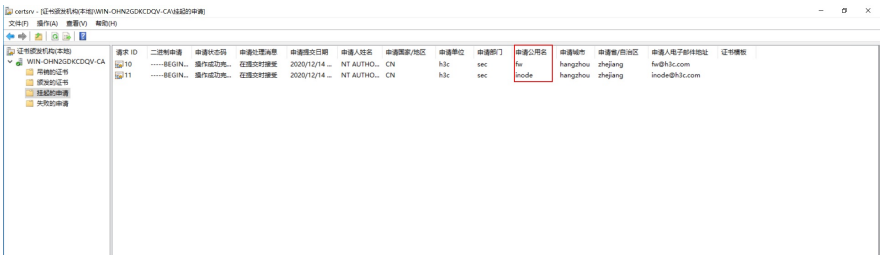


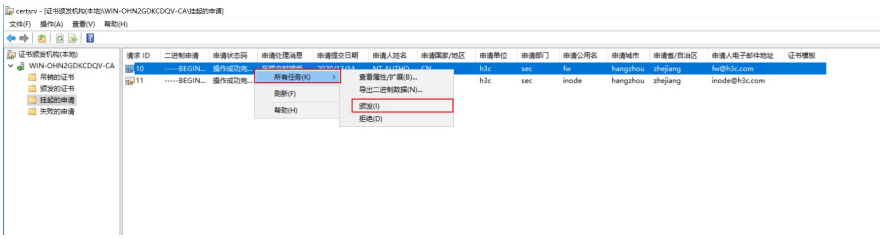
3， 同样的，重新打开证书服务链接， 这里申请SSL VPN客户端证书即iNode引用证书，**姓名(Common-Name)**设置为**inode**(和本地密码认证local-user相同name) ， 证书类型为**客户端身份验证证书**，并**标记密钥为可导出。**



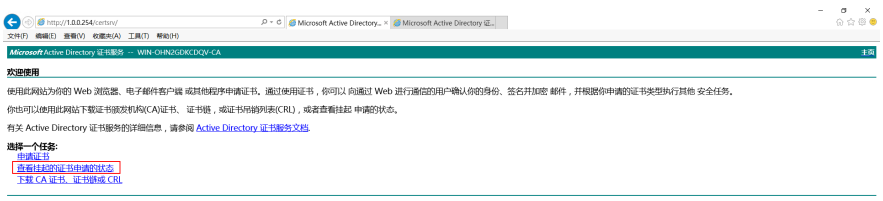


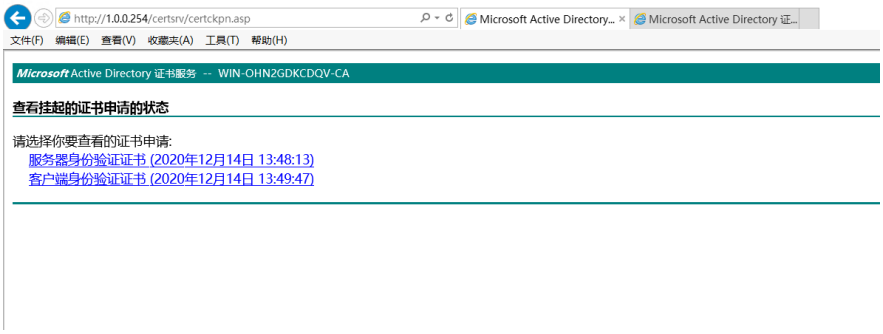
4，登入CA服务器桌面，在**证书颁发机构**中将申请的证书进行**颁发**。

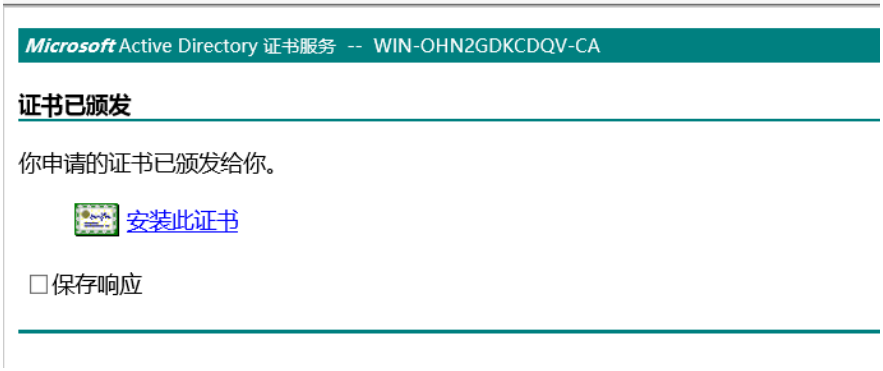


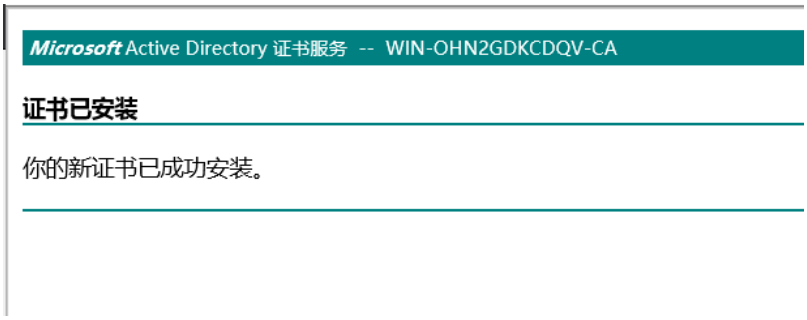


5， 重新在IE浏览器中打开证书服务链，**查看挂起的证书申请的状态**，**安装**之前申请的对应服务器证书和客户端证书。

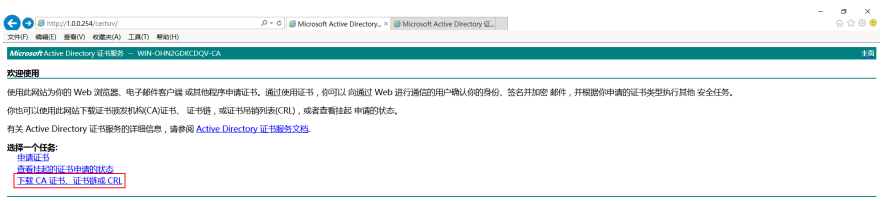


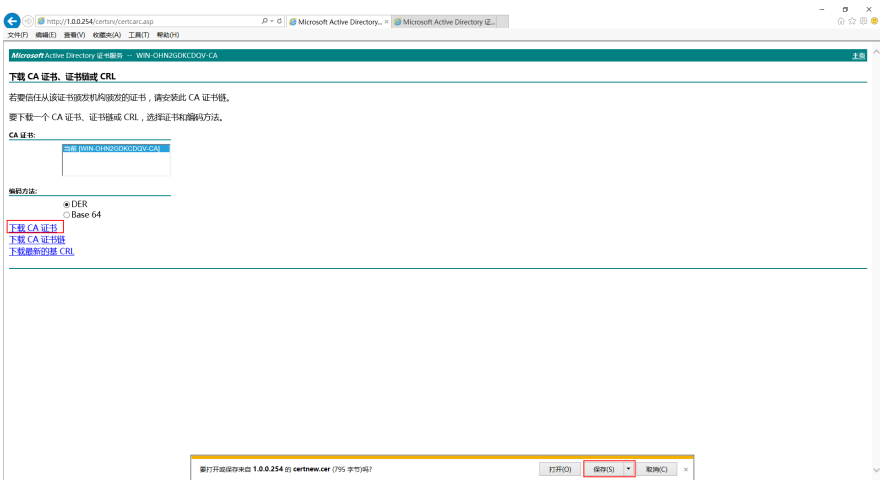


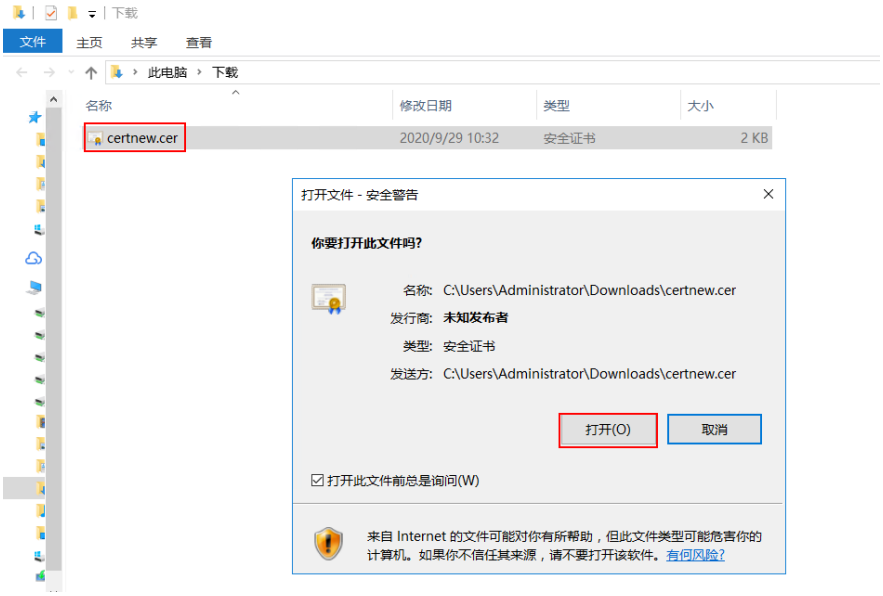




6，下载CA证书并**安装到受信任的根证书安装列表。**

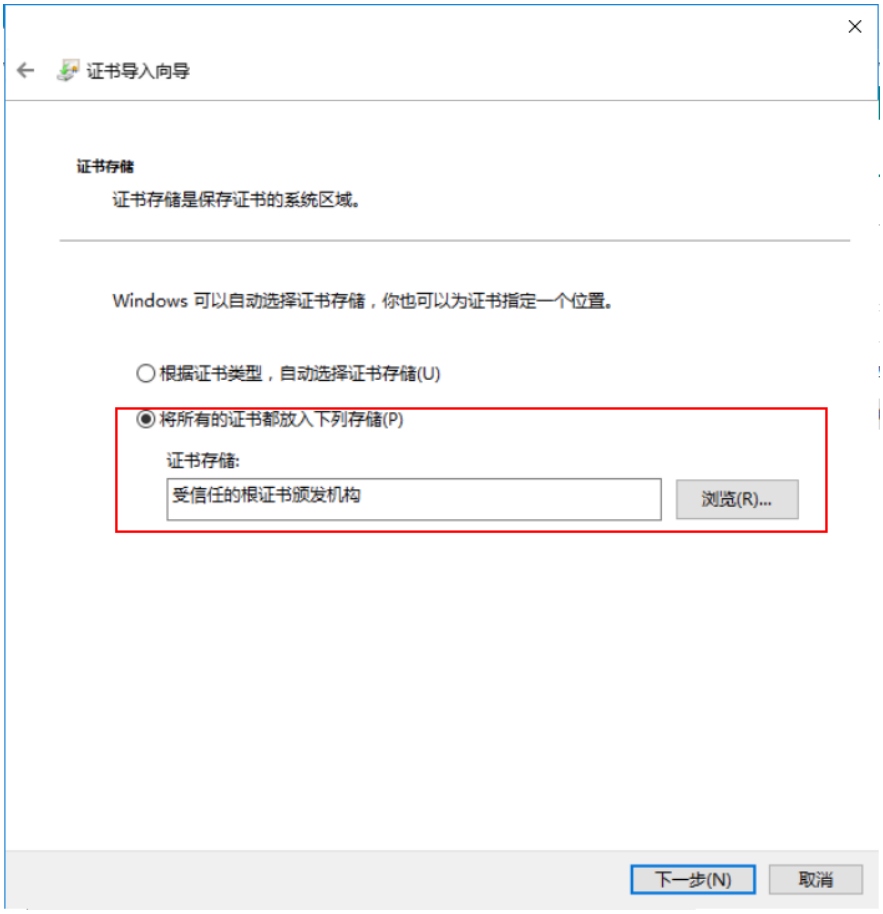


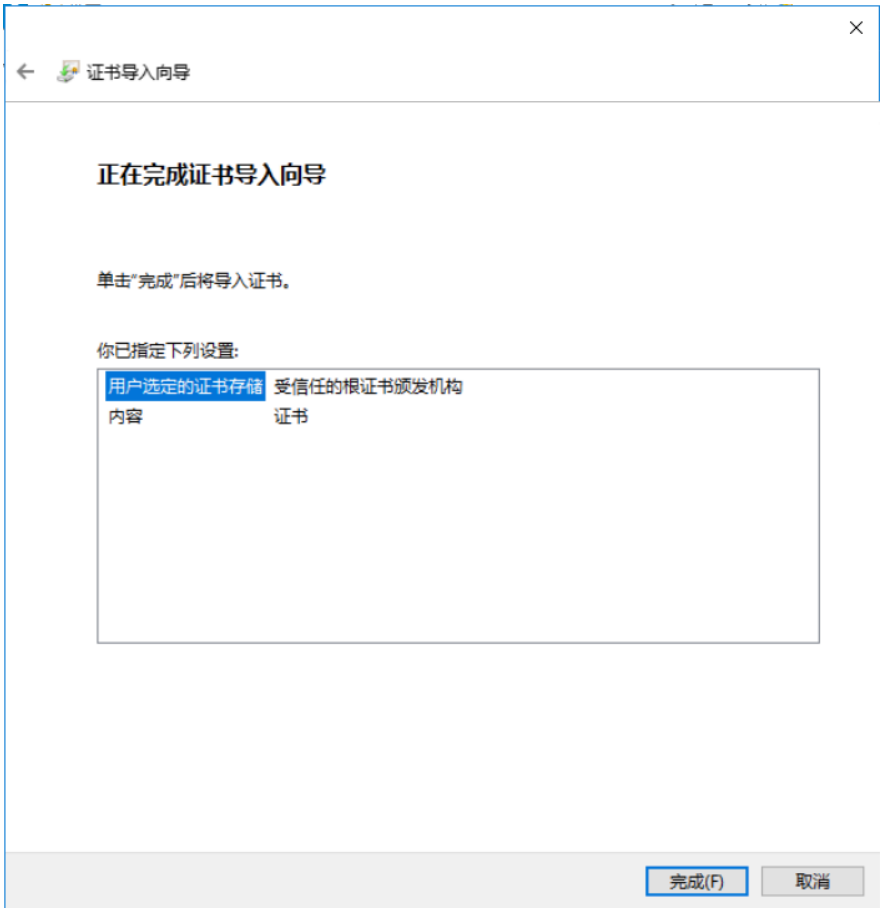

Microsoft Active Directory 证书服务 -- WIN-OHN2GDKCDQV-CA
下载 CA 证书、证书链或 CRL
若要信任从该证书颁发机构颁发的证书，请安装此 CA 证书链。
要下载一个 CA 证书、证书链或 CRL，选择证书和编码方法。
CA 证书:
编码方法:
DER
Base 64
下载 CA 证书
下载 CA 证书链
下载最新的基 CRL
打开(O)
保存(S)
取消(C)


下载
文件
主页
共享
查看
此电脑 › 下载
名称
修改日期
类型
大小
certnew.cer
2020/9/29 10:32
安全证书
2 KB
打开文件 - 安全警告
你要打开此文件吗?
名称: C:\Users\Administrator\Downloads\certnew.cer
发行商: 未知发布者
类型: 安全证书
发送方: C:\Users\Administrator\Downloads\certnew.cer
打开(O)
取消
打开此文件前总是询问(W)
来自 Internet 的文件可能对你有所帮助，但此文件类型可能危害你的计算机。如果你不信任其来源，请不要打开该软件。有何风险?

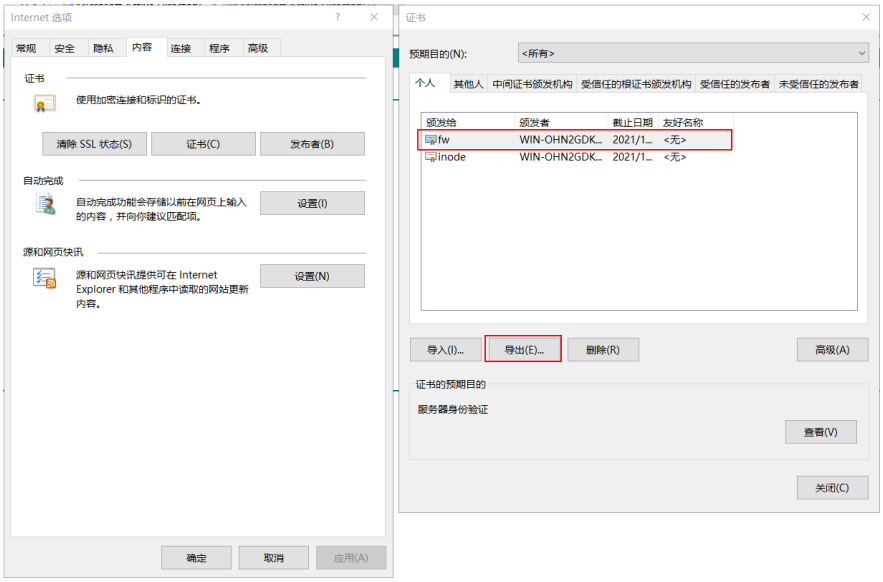

证书
常规
详细信息
证书路径
证书信息
这个证书的目的如下:
• 所有颁发策略
• 所有应用程序策略
颁发给: WIN-OHN2GDKCDQV-CA
颁发者: WIN-OHN2GDKCDQV-CA
有效期从 2020/12/9 到 2070/12/9
安装证书(I)...
颁发者说明(S)
确定

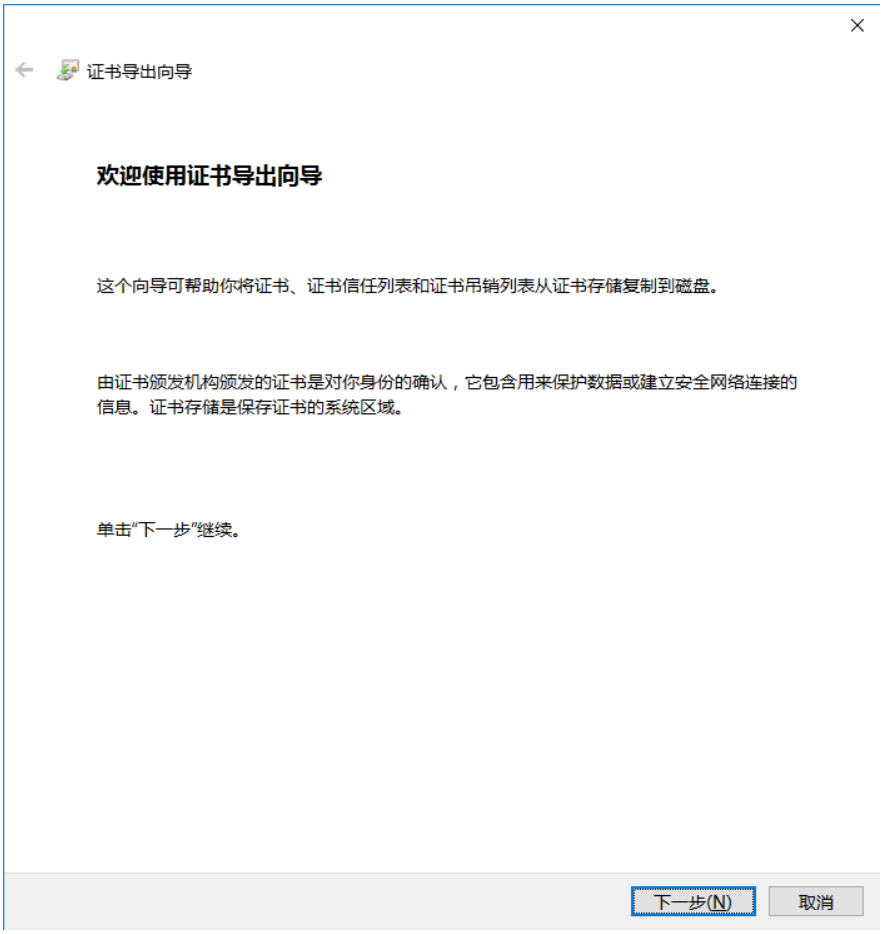

证书导入向导
欢迎使用证书导入向导
该向导可帮助你将证书、证书信任列表和证书吊销列表从磁盘复制到证书存储。
由证书颁发机构颁发的证书是对你身份的确认，它包含用来保护数据或建立安全网络连接的信息。证书存储是保存证书的系统区域。
存储位置
当前用户(C)
本地计算机(L)
单击"下一步"继续。
下一步(N)
取消

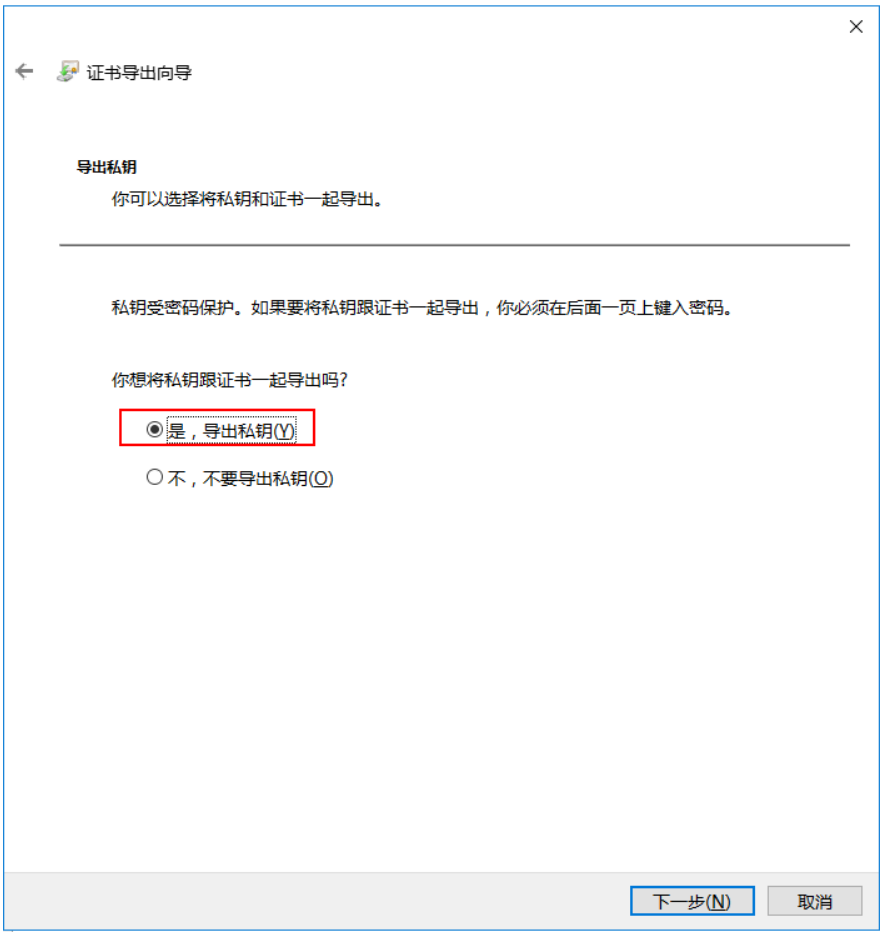


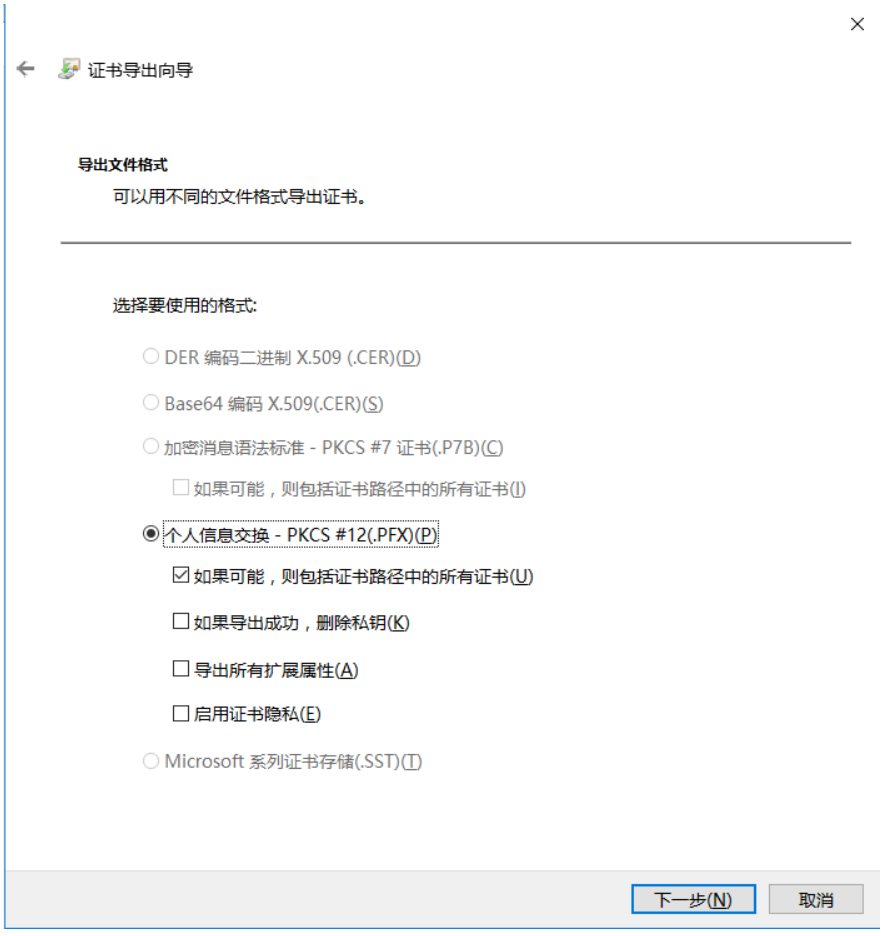


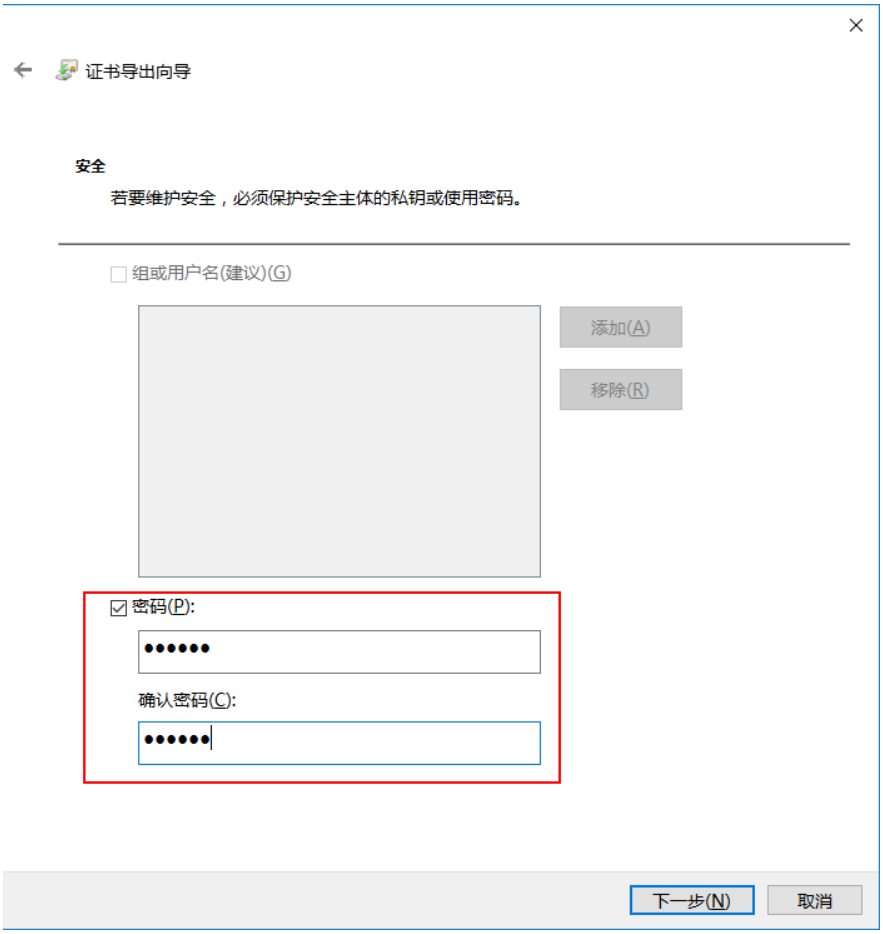
7，由于之前从CA申请的SSL VPN服务器证书和客户端证书都安装到了IE浏览器证书列表中，所以需要从IE浏览器导出服务器证书。

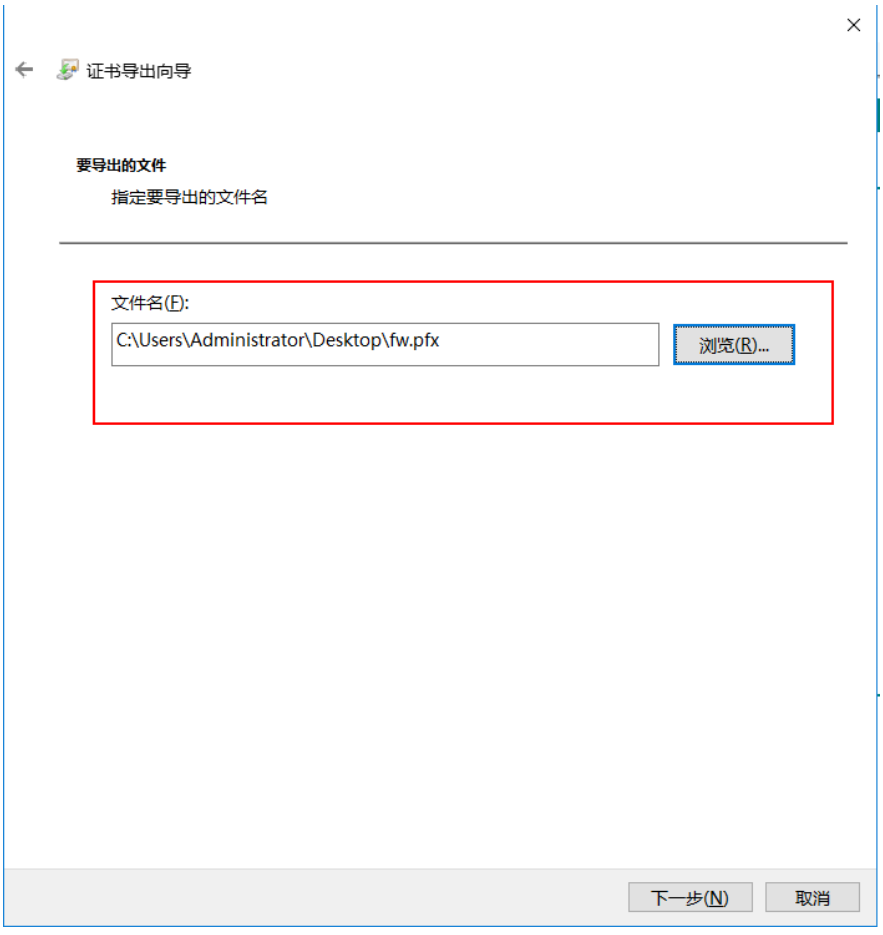

Internet 选项
常规
安全
隐私
内容
连接
程序
高级
证书
使用加密连接和标识的证书。
清除 SSL 状态(S)
证书(C)
发布者(B)
自动完成
自动完成功能会存储以前在网页上输入的内容，并向你建议匹配项。
设置(I)
源和网页快讯
源和网页快讯提供可在 Internet Explorer 和其他程序中读取的网站更新内容。
设置(N)
确定
取消
应用(A)
证书
预期目的(N):
<所有>
个人
其他人
中间证书颁发机构
受信任的根证书颁发机构
受信任的发布者
未受信任的发布者
颁发给
颁发者
截止日期
友好名称
fw
WIN-OHN2GDK...
2021/1...
<无>
inode
WIN-OHN2GDK...
2021/1...
<无>
导入(I)...
导出(E)...
删除(R)
高级(A)
证书的预期目的
服务器身份验证
查看(V)
关闭(C)

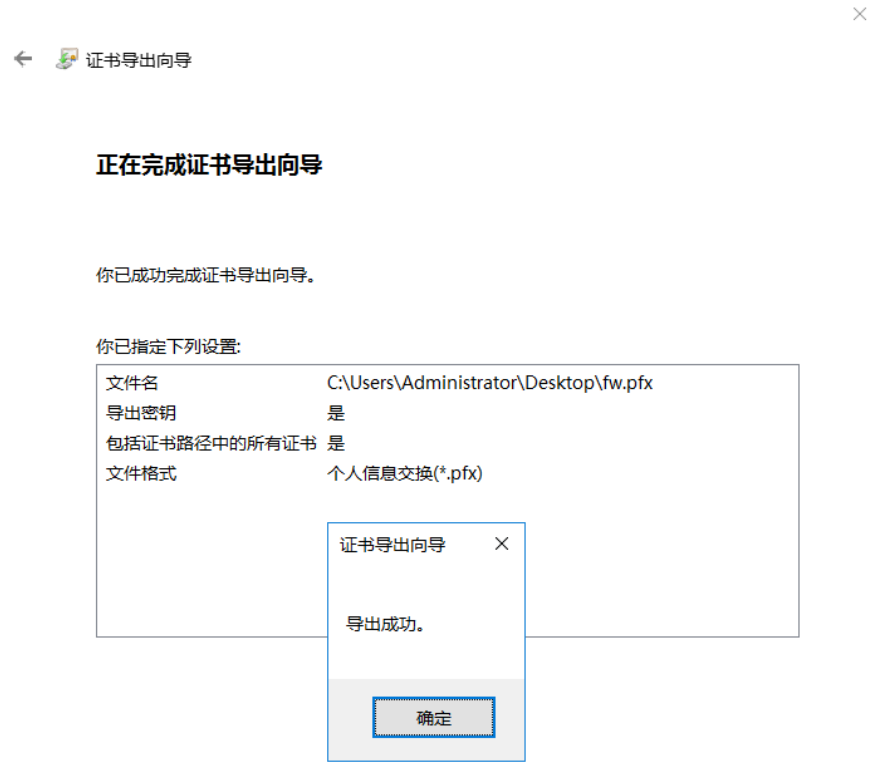

证书导出向导
欢迎使用证书导出向导
这个向导可帮助你将证书、证书信任列表和证书吊销列表从证书存储复制到磁盘。
由证书颁发机构颁发的证书是对你身份的确认，它包含用来保护数据或建立安全网络连接的信息。证书存储是保存证书的系统区域。
单击"下一步"继续。
下一步(N)
取消


证书导出向导
导出私钥
你可以选择将私钥和证书一起导出。
私钥受密码保护。如果要将私钥跟证书一起导出，你必须在后面一页上键入密码。
你想将私钥跟证书一起导出吗?
是，导出私钥(Y)
不，不要导出私钥(O)
下一步(N)
取消


证书导出向导
导出文件格式
可以用不同的文件格式导出证书。
选择要使用的格式:
DER 编码二进制 X.509 (.CER)(D)
Base64 编码 X.509(.CER)(S)
加密消息语法标准 - PKCS #7 证书(.P7B)(C)
如果可能，则包括证书路径中的所有证书(I)
个人信息交换 - PKCS #12(.PFX)(P)
如果可能，则包括证书路径中的所有证书(U)
如果导出成功，删除私钥(K)
导出所有扩展属性(A)
启用证书隐私(E)
Microsoft 系列证书存储(.SST)(T)
下一步(N)
取消


证书导出向导
安全
若要维护安全，必须保护安全主体的私钥或使用密码。
组或用户名(建议)(G)
添加(A)
移除(R)
密码(P):
确认密码(C):
下一步(N)
取消

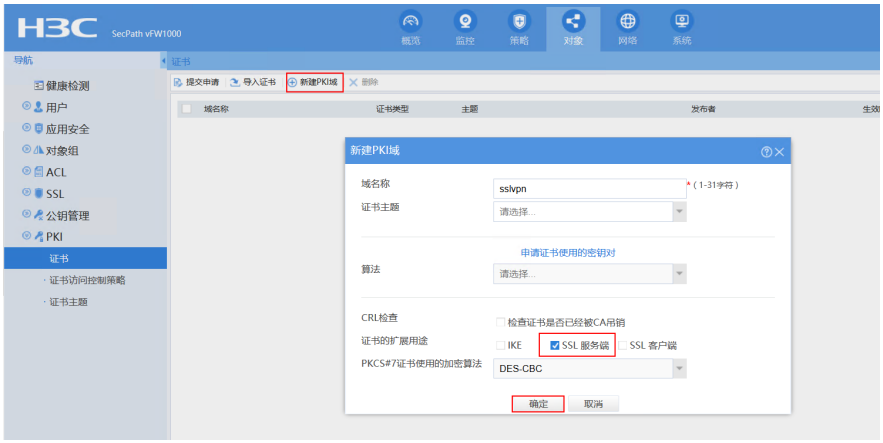

证书导出向导
要导出的文件
指定要导出的文件名
文件名(F):
C:\Users\Administrator\Desktop\fw.pfx
浏览(R)...
下一步(N)
取消

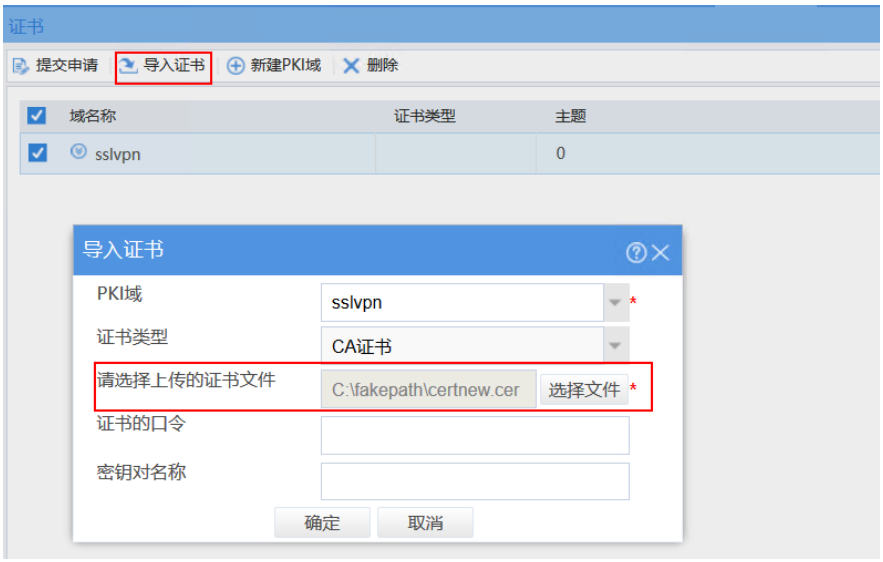


导出的SSL VPN服务器证书即为防火墙PKI模块中的本地证书，和之前下载的CA证书一同形成证书对。

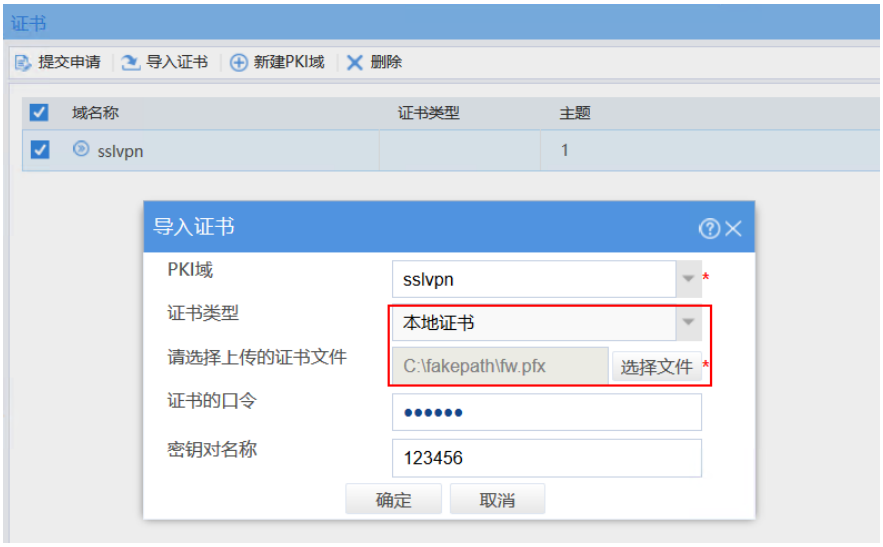
8，测试保证SSL VPN本地密码认证可以通过。

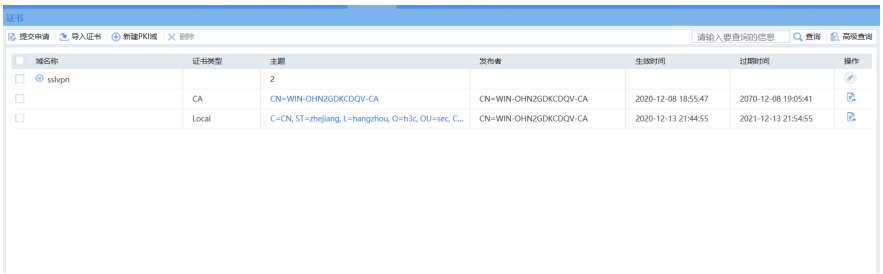
9，进入防火墙，新建PKI，分别导入CA证书和本地证书。



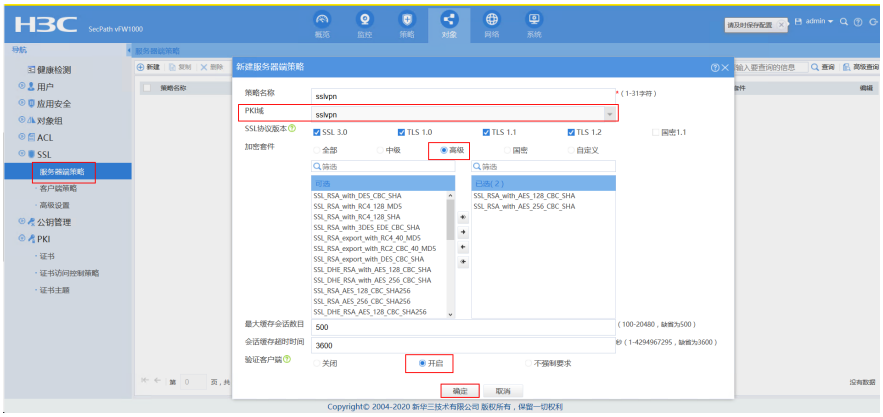


这里的证书口令为IE浏览器导出时设置的口令。

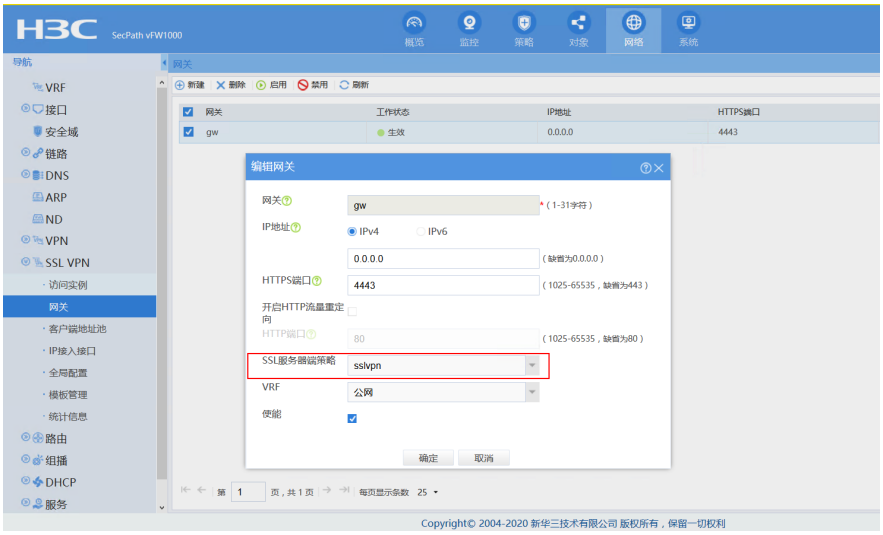


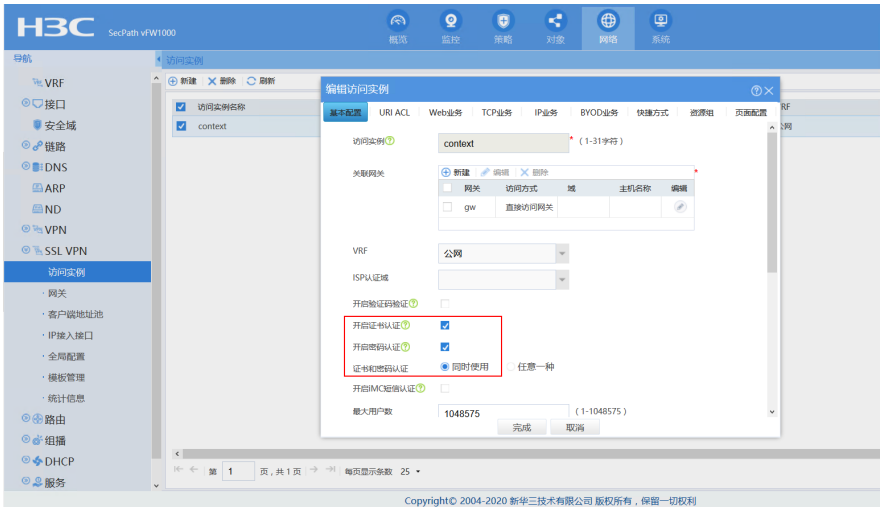


10，这里SSL服务器端策略引用对应的PKI域，选中高级加密套件（避免被扫描出算法漏洞），**注意一定要开启【验证客户端】。**



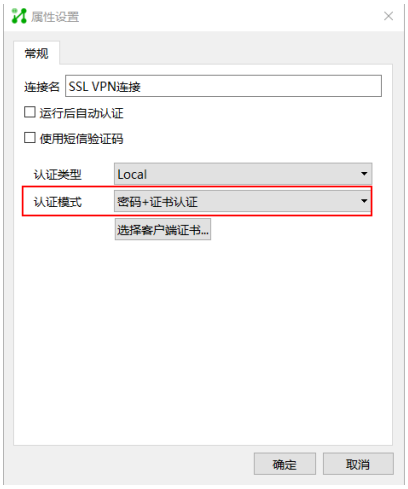
11，SSL VPN配置中，网关引用创建的SSL服务器端策略，并在访问实例中开启**证书和密码**同时使用。

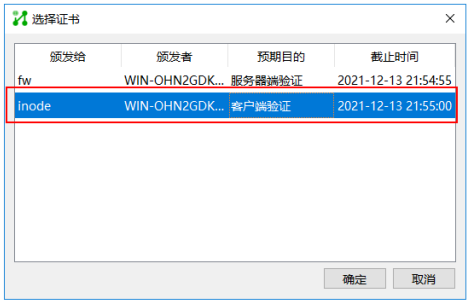




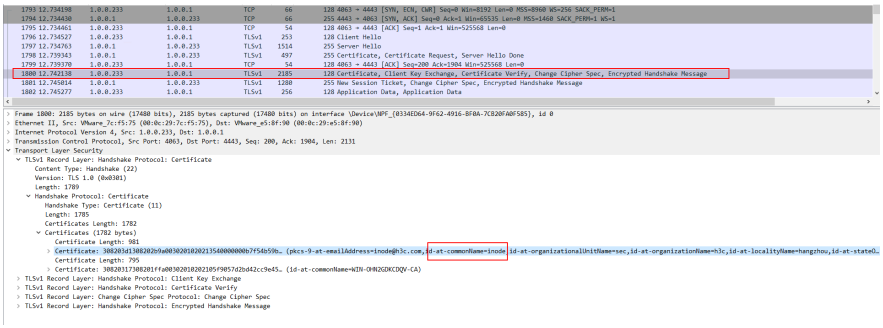
12，iNode设置认证模式为**密码+证书认证**，拨测可以成功，抓包可以看到SSL交互过程中iNode会发送客户端证书。


En
iNode智能客户端
SSL VPN连接
网 关
1.0.0.1:4443
用户名
inode
密 码
域
保存用户名
保存密码
连 接
属性...
我的场景


属性设置
常规
连接名
SSL VPN连接
运行后自动认证
使用短信验证码
认证类型
Local
认证模式
密码+证书认证
选择客户端证书...
确定
取消


选择证书
颁发给
颁发者
预期目的
截止时间
fw
WIN-OHN2GDK...
服务器端验证
2021-12-13 21:54:55
inode
WIN-OHN2GDK...
客户端验证
2021-12-13 21:55:00
确定
取消


En
iNode智能客户端
SSL VPN连接
网 关
1.0.0.1
当前用户
inode
域
无
安全状态
未检查
上线时间
2020-12-14 14:45:10
断 开
我的场景



以上，使用SSL VPN证书双向认证已顺利完成！

配置关键点

无