# 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 VP N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;
- ii 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。** 

< ) / http	p://1.0.0.254/certsrv/certrqma.asp	- C Similar Contractive Directory ×
文件(F) 编辑(E)	查看(V) 收藏夹(A) 工具(T) 帮助(H)	,
<b>吉你证书由注</b>		
向级业书中府		
识别信息:		
姓名:	: fw	
电子邮件:	; fw@h3c.com	
公司:	: h3c	
部门:	: SEC	
市/县:	hangzhou	
(1)	: zhejiang	
国家/地区:	: CN	
需要的证书类型:		_
	服务器身份验证证书 🗸	
密钥选项:		
	<ul> <li>创建新密钥集</li> <li>使用现存的密钥集</li> </ul>	-
CSP:	Microsoft RSA SChannel Cryptographic Provider	
密钥用法:	: ④ 交换	
密钥大小:	: 1024 量小值: 384 (一般密明大小: <u>512 1024 2048 4096 8192 16384</u> ) 最大值:16384	
	<ul> <li>自动密钥容器名称</li> <li>用户指定的密钥容器名称</li> </ul>	
	☑ 标记密钥为可导出	
	□ 启用强私钥保护	
其他选项:		_
申请格式:	CMC	
哈希算法:	sha1 🗸	
	仅用于申请签名。	
	□ 保存申请 	
屉性		
	< >	
好记的名称:	z	
		_
	提交 >	



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。** 

Comparison of the state of the	🖸 - د 🖉 🧭 Microsoft Active Directory تک 🍠 Microsoft Active Directory ×
文件(F) 编辑(E) 查看(V) 收藏夹(A) 工具(T) 帮助(H)	
Microsoft Active Directory 证书服务 WIN-OHN2GDKCDQV-CA	
高级证书申请	
识别信息:	
姓名: Inode	
电子邮件: inode@h3c.com	
公司: h3c 部门: sec	
市/县: hangzhou	
省: zhejiang	
国家/地区:   cn	
<b>需要的证书类型:</b>	-
<b>廖</b> 田洗面:	
<ul> <li>● 创建新密钥集 ○ 使用现存的密钥集</li> </ul>	-
CSP: Microsoft RSA SChannel Cryptographic Provider	$\overline{}$
密胡用法: ◉ 交換	
密钥入小: 1024 最大图:16384 (一般商用大小: 512 1024 2048 8192 16384) ● 自动密相查器名称 ○ 用户指示的密相查器名称	
☑ 标记密钥为可导出	
□ 启用强私钥保护	
其他选项:	_
申请格式: ○ CMC ● PKCS10	
暗希算法: sha1 ✓ <i>仅用于申请签答。</i>	
□保存申请	
<b>屋性:</b>	
好记的名称:	
提交 >	
	,
← ( ) Ø http://1.0.0.254/certsrv/certfnsh.asp	・ ク マ C / @ Microsoft Active Directory 证 / @ Microsoft Active Directory ×
文件(F) 编辑(E) 查看(V) 收藏夹(A) 工具(T) 帮助(H)	
Microsoft Active Directory 证书服务 WIN-OHN2GDKCDQV-CA	
证书正在持起	
初初班书申请已经收到。但是,初必须守侍官理贞观反称申请的	ист».
10月1日の1月1日。	
请在一天或两天内返回此网站以检索你的证书。	
注意: 你必须用此 Web 浏览器在 10 天内返回才能检察你的证书	

#### 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。**



🙀 certe	rv - (证书级发机构(本地)\WIN	-OHN2GDK	CDQV-CA	(中语)												
文件(F)	损作(A) 查撒(V) 帮助	(H)														
<b>*</b> *	2 🙆 🔒 👔															
(2) (2)	5.疲发机构(本地)	请求 ID	二进制申请	申请状态码	申请处理消息	申请提交日期	申请人姓名	申请国家/地区	申请单位	申请郎门	申请公用名	由遺城市	申请省/自治区	申请人电子邮件地址	证书模板	
~ al	WIN-OHN2GDKCDQV-CA	<b>10</b>	BEGIN	操作成功完	total contractions.	2020/12/14	NT AUTHO	CN	h3c	sec	fw	hangzhou	zhejiang	fw@h3c.com		
	1 100000000000000000000000000000000000	11	·····BEGIN	操作成功完	所用性肉(N)	,	11-11-11-11-11-11-11-11-11-11-11-11-11-		h3c	sec	inode	hangzhou	zhejiang	inode@h3c.com		
	1 挂起的申请				用则制(F)		2898/0									
1	关致的申请				和3的(H)		おこの(I) 拒絶(D)									
1																
E	まったに		se da tr	र रागः स	十三方	<u>たた</u> Z	5=+±:	はわわいて	++ cb.%	主人人	上大		ンボー	きんちっきょう	吧夕日	いた
э,	里利住口	끼꼬	品计了	コエモ	口服分	挺, 重	ショクチョン	FEBANC.	ויייס	8074	، ٽڪ َ، ٨	又衣	く同中	旧ロコンコレプ	加入之子	러면 다

和客户端证书。

	- 5 × @\$\$
Microsoft Active Directory 证书题版 WIN-OHN2GDKCDQV-CA	主页
<b>欢迎使用</b>	
使用组织起力你的"Web 湖底器"。电子和件数字编 或其他相对中央而正书、通过使用正书,你可以 的通过 Web 进行通信控用中级从你的角份。答名开加密 邮件,开稿路向中做的证书来型的正书来型的工程他 安全任务。 你也可以应用此现象指于和这一性组成和如《VLEF、 证书报,或证书和确知来CRU,或者是像目起 中面的状态。 教术 Anton Encercor 证书服务的详细信息,请参照 Active Directory 证书服务文化 图 <mark>算一个155:</mark>	
Reflection towards.	

← ⊕ Ø http://1.0.0.254/certsrv/certckpn.asp	P ▼ C G Microsoft Active Directory × G Microsoft Active Directory 证
文件(F) 編輯(E) 查看(V) 收藏夹(A) 工具(T) 帮助(H)	
Microsoft Active Directory 证书服务 WIN-OHN2GDKCDQV-CA	
查看挂起的证书申请的状态	
请选择你要查看的证书申请:	
服务器身份验证证书 (2020年12月14日 13:48:13) 客户端身份验证证书 (2020年12月14日 13:49:47)	

Microsoft Active Directory 证书服务 -- WIN-OHN2GDKCDQV-CA

## 证书已颁发

你申请的证书已颁发给你。

🔛 安装此证书

□保存响应

*Microsoft* Active Directory 证书服务 -- WIN-OHN2GDKCDQV-CA

## 证书已安装

你的新证书已成功安装。

6, 下载CA证书并**安装到受信任的根证书安装列表**。

( ) ( mm//1.82244/cmtn/) アーク ( ) Microsoft Active Directory. × ( Microsoft Active Directory ().     ( 対応ののft Active Directory ().     ( 対応ののft Active Directory ().	- ♂ × @ ☆ ⊕ ●
Alicrosoft Active Directory IE-H885 WIN-OHN26DKCDQV-CA	主页
大迎使用	
便用此网站为你的 Web 浏览器、电子邮件客户端 或其他程序申请证书,通过使用证书,你可以 向通过 Web 进行漏信的用户输认你的身份、签名并加密 邮件,并根据你申请的证书类型均行其他 安全任务。	
你也可以他用此网站下载证书服装机构(CA)证书、证书册,或证书用物列表(CRL),或者查看挂起申请的状态。	
有关 Active Directory 证书服务的详细信息,请参阅 Active Directory 证书服务文档。	
<b>送降 一代表:</b> 由詞記書 資料は2012年1月1日前代は志 <u> 下載 (A 近年、近半時頃</u> (R)]	

Mittp://100254/certsrv/certcarc.asp	P - 0	Microsoft Active Directory ×	JMicrosoft Active Directory (Z.,			- σ × ⊙☆©9
soft Active Directory 证书服务 WIN-OHN2GD	KCDQV-CA					±8 ^
A 证书、证书辅或 CRL						
在从该证书颁发机构颁发的证书,请安装此	CA 证书链。					
一个 CA 证书、证书继或 CRL,选择证书和	瘤码方法.					
mill [win-ohnzgdkcdqv-ca]						
<u>k</u>						
DER     Base 64						
A 证书辦 A 证书辦						
MILSIE C.KL						_
	要打开或保存来自 1.0.0.254 的	certnew.cer (795 李竹)吗?		打开(O) 保存(S) • 取(的(C)	×	~
					1	
🖸 📕 -   下恭						
¥   <del>•</del> • <u>•</u> <u>•</u> <u>•</u>						
牛 主页 共享	查看					
	ⅰ 〉 下戦					
→ ↑ ↑ ↓ ・ 此电脑 ▲ 名称	i > 下载 ^		修改日期	类型	大小	
→ · ↑ · 此电脑 <sup>▲</sup> 名称	i > 下载 ^		修改日期	大型	大小	
→ · ↑ ▶ · 此电脑 <sup>^</sup> 名称 <sup>_</sup> Certnew.cer	5.) 下载 ^		修改日期 2020/9/29 10:32	<b>类型</b> 安全证书	大小 2 KB	
→ · ↑ · 此电脑 合称 「 certnew.cer	i > 下载 ^		修改日期 2020/9/29 10:32	<b>类型</b> 安全证书	大小 2 KB	
→ 、 个 → 此电脑 へ 名称 。 certnew.cer	ā→ 下戦 へ	打开文件 - 安全	修改日期 2020/9/29 10:32 警告	关型 安全证书	大小 2 KB ×	
→ 个 小 此电脑 合称 Grant Certnew.cer	i > 下载 	打开文件 - 安全	修改日期 2020/9/29 10:32 警告	类型 安全证书	大小 2 KB ×	
→ 个 <b>▶</b> 此电脑 合称 G称 Certnew.cer	i > 下载 	打开文件 - 安全 你要打开此文(	修改日期 2020/9/29 10:32 警告 件¥9 <b>?</b>	关型 安全证书	大小 2 KB X	
→ 、 ↑ → ▲ 合称 a certnew.cer	i > 下载 ^	打开文件 - 安全 <b>你要打开此文(</b>	修改日期 2020/9/29 10:32 警告 <b>件时</b> ?	<b>类型</b> 安全证书	大小 2 KB ×	
→ 、 ↑ ▶ 此电脑 へ 名称 に certnew.cer	ī > 下载 ^	打开文件 - 安全 你要打开此文(	修改日期 2020/9/29 10:32 警告 件吗? 名称 C:\Users\Admi	关型 安全证书	大小 2 KB ×	
→ ↑↑ ▶→ 此电脑 ↑ 名称 ↓ Certnew.cer	i > 下戦 ^	打开文件 - 安全 <b>你要打开此文</b> 化	修改日期 2020/9/29 10:32 警告 年期3 名称 C:\Users\Admin 世行帝 年期264章	类型 安全证书 nistrator\Downloads\c	大小 2 KB ×	
→ 个 ▶ 此电脑 へ 名称 。 certnew.cer	i > 下戦 ^	打开文件 - 安全 <b>你要打开此文</b> 化 译	修改日期 2020/9/29 10:32 警告 <b>件吗?</b> 名称: C:\Users\Admi 发行商: <b>未知发布者</b>	美型 安全证书 nistrator\Downloads\c	大小 2 KB × ertnew.cer	
→ 个 ▶ 此电脑	i > 下载 ^	打开文件 - 安全 你要打开此文( 。	修改日期 2020/9/29 10:32 警告 <b>件时?</b> 名称 C:\Users\Admi 发行商: <b>未知发布者</b> 类型:安全证书	送型 安全证书 nistrator\Downloads\co	大小 2 KB × ertnew.cer	
→ 、 ↑ ▲ 合称 ▲ Certnew.cer	i > 下载 ^	打开文件 - 安全 你要打开此文( 。 ;	修改日期 2020/9/29 10:32 警告 件吗? 名称: C:\Users\Admin 发行商: <b>未知发布者</b> 类型: 安全证书 发送方: C:\Users\Admin	类型 安全证书 nistrator\Downloads\c nistrator\Downloads\c	大小 2 KB × ertnew.cer	
→ 、 ↑ → 此电融 へ 名称 Gara certnew.cer	i > 下戦 ^	打开文件 - 安全 <b>你要打开此文(</b> 。 。 。 。 。	修改日期 2020/9/29 10:32 警告 件19? 在称 C:\Users\Admi 发行商: <b>未知发布者</b> 类型: 安全证书 发送方: C:\Users\Admi	美型 安全证书 nistrator\Downloads\co	大小 2 KB × ertnew.cer	
→ 、 ↑ ▲ → 此电融 へ 名称 Garacertnew.cer	i > 下戦 ^	打开文件 - 安全 <b>你要打开此文(</b> []] ; ;	修改日期 2020/9/29 10:32 警告 件码? 名称 C:\Users\Admin 发行商: 未知发布者 类型: 安全证书 发送方: C:\Users\Admin	美型 安全证书 nistrator\Downloads\cc nistrator\Downloads\cc	大小 2 KB × ertnew.cer ertnew.cer	
→ · ↑ → 此电融 A 名称 G certnew.cer	i > 下戦 ^	打开文件 - 安全 <b>你要打开此文(</b> 。 ;	修改日期 2020/9/29 10:32 警告 <b>件吗?</b> 名称 C:\Users\Admin 发行簿: <b>未知发布者</b> 类型: 安全证书 发送方: C:\Users\Admin	美型 安全证书 nistrator\Downloads\c nistrator\Downloads\c 打开(O)	大小 2 KB × ertnew.cer ertnew.cer	
→ 、 ↑ ▲ → 此电起 A 名称 a certnew.cer	i > 下载 ^	打开文件 - 安全 <b>你要打开此文</b> ( 。 ; ;	修改日期 2020/9/29 10:32 警告 <b>件吗?</b> 名称: C:\Users\Admi 发行商: <b>未知发布音</b> 类型: 安全证书 发送方: C:\Users\Admi	类型 安全证书 nistrator\Downloads\c nistrator\Downloads\c 打开(O)	大小 2 KB × ertnew.cer ertnew.cer 取消	
→ · · ↑ ▲ · 此电融 A 名称 G a certnew.cer	i > 下载 ^	打开文件 - 安全 <b>你要打开此文(</b> ; ; ; ; ; ; ;	修改日期 2020/9/29 10:32 警告 <b>件吗?</b> 名称: C:\Users\Admi 发行商: <b>未知发布者</b> 类型: 安全证书 发送方: C:\Users\Admi	类型 安全证书 nistrator\Downloads\c nistrator\Downloads\c 打开(O)	大小 2 KB × ertnew.cer ertnew.cer 取消	
→ · ↑	i > 下载 ^	打开文件 - 安全 <b>你要打开此文(</b> 〕 □ □ 打开此文件	修改日期 2020/9/29 10:32 <b>容許</b> <b>件明?</b> 在称 C:\Users\Admi 发行商: <b>未知发布者</b> 类型: 安全证书 发送方: C:\Users\Admi	美型 安全证书 nistrator\Downloads\c nistrator\Downloads\c 打开(O)	大小 2 KB ertnew.cer ertnew.cer 取消	
→ · ↑ → 此电融 へ 名称 Gar Certnew.cer	i > 下戦 ^	打开文件 - 安全 <b>你要打开此文(</b> □ □ □ 打开此文件	修改日期 2020/9/29 10:32 警告 件明? 在称 C:\Users\Admi 发行商: <b>未知发布者</b> 樂型: 安全证书 发送方: C:\Users\Admi 前忠是询问(W)	美型 安全证书 nistrator\Downloads\c 打开(O) 次有所帮助、但以文件 挙	大小 2 KB × ertnew.cer 取消	
→ · ↑ → 此电融	i > 下载 ^	打开文件 - 安全 <b>你要打开此文(</b> □ □ 打开此文件 ¥ 間 计算	修改日期 2020/9/29 10:32 警告 <b>件吗?</b> 名称: C:\Users\Admin 发行商: <b>未知发布者</b> 类型: 安全证书 发送方: C:\Users\Admin 前总是询问(W) Internet 的文件可能对; 机, 如果你不信任某类测	美型 安全证书 nistrator\Downloads\cc nistrator\Downloads\cc 打开(O) 尔有所帮助,但此文件类 『 请不要打开该软件。 #	大小 2 KB × ertnew.cer ertnew.cer 取消 型可能危害你的	

证书	×
详细信息 证书路径	
(正书信自)	
12 Mar 12 1947CA	
这个证书的目的如下:	
<ul> <li>所有</li></ul>	
IRSCH. WIN-OHNZODKEDQV-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)
--------

×

. \$. Mudalina	
证书存储	
证书存储是保存证书的系统区域。	
Windows 可以自动选择证书存储,你也可以为证书指	定一个位置。
○根据证书类型,自动选择证书存储(U)	
●将所有的证书都放入下列存储(P)	
证书存储:	
受信任的根证书颁发机构	浏览(R)
	M320(rt)
	ト一步(N) 取消
	· · · · · · · · · · · · · · · · · · ·
🍠 证书导入向导	
🌮 证书导入向导	
🊰 证书导入向导	
ジ 证书导入向导 正在完成证书导入向导	
<i>疑</i> 亚书导入向导 <b>正在完成证书导入向导</b>	
✓ 证书导入向导 正在完成证书导入向导 单击"言动"后终导入证书	
证书导入向导 正在完成证书导入向导 单击"完成"后将导入证书。	
证书导入向导 正在完成证书导入向导 单击"完成"后将导入证书。	
<ul> <li>证书导入向导</li> <li>正在完成证书导入向导</li> <li>单击"完成"后将导入证书。</li> <li>你已指定下列设置:</li> </ul>	
✓ 证书导入向导 正在完成证书导入向导 单击"完成"后将导入证书。 你已指定下列设置: 用户选定的证书存储 受信任的根证书颁发机构 工者	
<ul> <li>亚书导入向导</li> <li>正在完成证书导入向导</li> <li>单击"完成"后将导入证书。</li> <li>你已指定下列设置:</li> <li>用户选定的证书存储 受信任的根证书颁发机构 内容 证书</li> </ul>	
<ul> <li>亚书导入向导</li> <li>正在完成证书导入向导</li> <li>单击"完成"后将导入证书。</li> <li>你已指定下列设置:         <ul> <li>用户选定的证书存储</li> <li>受信任的根证书颁发机构</li> <li>内容</li> <li>证书</li> </ul> </li> </ul>	
<ul> <li>证书导入向导</li> <li>正在完成证书导入向导</li> <li>单击"完成"后将导入证书。</li> <li>你已指定下列设置:</li> <li>用户选定的证书存储 受信任的根证书颁发机构 内容 证书</li> </ul>	
证书导入向导 正在完成证书导入向导 单击"完成"后将导入证书。 你已指定下列设置: 用户选定的证书存储 受信任的根证书颁发机构 证书	
亚书导入向导 正在完成证书与入向导 单击"完成"后将导入证书。 你已指定下列设置: 用户选定的证书存储 受信任的根证书颁发机构内容 证书	
✓ 证书导入向导          正在完成证书导入向导         単击"完成"后将导入证书。         你已指定下列设置:         用户选定的证书存储       受信任的根证书颁发机构         内容       证书	
✓ 证书导入向导 正在完成证书导入向导 单击"完成"后将导入证书。 你已指定下列设置: 用户选定的证书存储 受信任的根证书颁发机构 内容 证书	
✓ 证书导入向导          正在完成证书导入向导         单击"完成"后将导入证书。         你已指定下列设置:         用户选定的证书存储       受信任的根证书颁发机构         内容       证书	
✓ 证书导入向导          正在完成证书导入向导         单击"完成"后将导入证书。         你已指定下列设置:         用户选定的证书存储       受信任的根证书颁发机构         内容       证书	
ション・ション・ション・ション・ション・ション・ション・ション・ション・ション・	
正在完成证书导入向导           单击"完成"后将导入证书。           PE指定下列设置:           用户选定的证书存储         受信任的根证书颁发机构           内容         证书	
正在完成证书导入向导           单本"完成"后将导入证书。           你已指定下列设置:           用户选定的证书存储         受信任的根证书颁发机构           内容<	
▼ 証书导入向导  広在完成证书与入向与  単本"完成"后将导入证书、 の円指定下列设置:   四一方选定的证书存储 受信任的根证书颁发机构 内容 近书	
● 正书与入向导 正在完成证书与入向与 単本"完成"后将导入证书。 の已指定下列设置: 用户选定的证书存储 受信任的根证书颁发机构 内容 近书	

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。

	× [ 证书
N 安全 隐私 内容 连接 程序 高级	- 预期目的(N):
*	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
e用加密连接和标识的证书。	
(8)素式伏 (2)朱秋 [22 領部	
	□□ Inode WIN-OHN2GDK 2021/1 <无>
新 自动与此约为此为开始采用的工作的文工和八 读直(1) 的内容,并向你建议匹配项。	
0网页快讯	
源和网页快讯提供可在 Internet 设置(N)	
內容。	
	(I) (YCI) 開除(K) (m)扱(A)
	证书的预期目的
	服务器身份验证 查要0.0
	半途の
	×107(0)
确定 取消 应用(A	J
欢迎使用证书导出向导	
次迎使用证书导出向导	千列表和证书吊销列表从证书存储复制到磁盘。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信何	任列表和证书吊销列表从证书存储复制到磁盘。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付	任列表和证书吊销列表从证书存储复制到磁盘。 自必的通过 - 它句今田本/8-10数据或建立字全网络连续的
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你 信息。证书存储是保存证书的系统	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认 , 它包含用来保护数据或建立安全网络连接的 X城。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信何 由证书颁发机构颁发的证书是对你引 信息。证书存储是保存证书的系统配	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认,它包含用来保护数据或建立安全网络连接的 区域。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你引 信息。证书存储是保存证书的系统[	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认,它包含用来保护数据或建立安全网络连接的 区域。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你引 信息。证书存储是保存证书的系统[	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认 , 它包含用来保护数据或建立安全网络连接的 区域。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你引 信息。证书存储是保存证书的系统配 单击"下一步"继续。	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认,它包含用来保护数据或建立安全网络连接的 区域。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你归 信息。证书存储是保存证书的系统团 单击"下一步"继续。	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认 , 它包含用来保护数据或建立安全网络连接的 区域。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你引 信息,证书存储是保存证书的系统证 单击"下一步"继续。	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认 , 它包含用来保护数据或建立安全网络连接的 区域。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你引 信息。证书存储是保存证书的系统证 单击"下一步"继续。	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认 , 它包含用来保护数据或建立安全网络连接的 区域。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你引 信息。证书存储是保存证书的系统证 单击"下一步"继续。	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认 , 它包含用来保护数据或建立安全网络连接的 区域。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你引 信息。证书存储是保存证书的系统配 单击"下一步"继续。	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认 , 它包含用来保护数据或建立安全网络连接的 ⊠域。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你引 信息。证书存储是保存证书的系统证 单击"下一步"继续。	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认 , 它包含用来保护数据或建立安全网络连接的 ⊠域。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你引 信息。证书存储是保存证书的系统证 单击"下一步"继续。	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认,它包含用来保护数据或建立安全网络连接的 ⊠域。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你引 信息。证书存储是保存证书的系统证 单击"下一步"继续。	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认,它包含用来保护数据或建立安全网络连接的 ⊠域。
<b>欢迎使用证书导出向导</b> 这个向导可帮助你将证书、证书信付 由证书颁发机构颁发的证书是对你引 信息。证书存储是保存证书的系统。 单击"下一步"继续。	任列表和证书吊销列表从证书存储复制到磁盘。 身份的确认,它包含用来保护数据或建立安全网络连接的 ⊠域。

	×
÷	₽ 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()
	下————————————————————————————————————
,	X
÷	⅔ 近书号田同号
	<b>导出文件格式</b> 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)( <u>S</u> )
	○ 加密消息语法标准 - PKCS #7 证书(.P7B)( <u>C</u> )
	□ 如果可能,则包括证书路径中的所有证书(l) 
	● 个人信息交换 - PKCS #12(.PFX)(P)
	□ 如果可能,则包括证书路径甲的所有证书(U)
	○ Microsoft 系列证书存储(.SST)①

下一步(<u>N</u>) 取消

÷	征书合用向导	×
T		
	<b>安全</b> 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(民)	
	一 或亚/D)・	
	✓ ₩H(F).	
	确认密码( <u>C</u> ):	
	•••••	
	下一步(N) 取消	
÷	☞ 证书导出向导	×,
	<b>要导出的文件</b> 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	

🗧 😼 证书导出向导

## 正在完成证书导出向导

你已成功完成证书导出向导。

文件名	C:\Users\Administrator\Desktop\fw.pfx	
导出密钥	是	
包括证书路径中的所有	正书 是	
文件格式	个人信息交换(*.pfx)	
	证书导出向导 ×	
	导出成功。	
	确定	

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。

完成(F) 取消

HBC SecPath vFW1	000	R H		() 策略	<b>く</b> 対象	网络	<b>望</b> 系统		
导航									
記健康检测	🕟 提交申请 🗨 导入证书 🧃	新建PKI城 × 新除							
💿 💄 用户	域名称	证书类型	主题				发布者		生效
💿 🟮 应用安全									
◎ 小 对象组		新建PKI域						@×	
💿 🚍 ACL		14 CT 10							
🗵 🛢 SSL		成古林		sslvpn			*(1-319973)		
💿 🦧 公钥管理		征书王牌		请选择			Ψ.		
💿 者 РКІ									
证书		簡注		申请	证书使用的密	钥对			
·证书访问控制策略		318724		请选择			Ť		
·证书主题									
		CRL检查		□ 检查证书	书是否已经被(	A吊销			
		证书的扩展	利途	🗌 IKE	☑ SSL 服务	i端 🗌 SSL 著	客户端		
		PKCS#7证书	6使用的加密算法	DES-CBC	;		÷		
				确)	定 取i	6			

ù	E书					
	) 提交	2 导入证书	🕀 新建PKI域 🗙 🖁	削除		
	<	域名称		证书类型	主题	
		sslvpn			0	

导入证书		$@\times$
PKI域	sslvpn	*
证书类型	CA证书	*
请选择上传的证书文件	C:\fakepath\certnew.cer	选择文件 *
证书的口令		
密钥对名称		
确	定 取消	

这里的证书口令为IE浏览器导出时设置的口令。

证书						
🚯 提交申请 🛛 🔁	,导入证书   🕀 新建PKI域   🗙 🗄	删除				
✓ 域名称		证书类型	主题			
sslvpr	n		1			
	导入证书				$@\times$	
	PKI域	sslvpn		~	*	
	证书类型	本地证书		~	1	
	请选择上传的证书文件	C:\fakepath\fw.pf	x	选择文件	*	
	证书的口令	•••••				
	密钥对名称	123456				
		确定 取消			_	

提交申请 🔰 导入证书 🕒 銅	LePKII或 × 删除			请输入	要查询的信息 🔍 童祹	🔒 高級重
城名称	证书类型	主题	发布者	生效时间	过期时间	操作
💿 sslvpn		2				Ø
	CA	CN=WIN-OHN2GDKCDQV-CA	CN=WIN-OHN2GDKCDQV-CA	2020-12-08 18:55:47	2070-12-08 19:05:41	R,
	Local	C=CN, ST=zhejlang, L=hangzhou, O=h3c, OU=sec, C	CN=WIN-OHN2GDKCDQV-CA	2020-12-13 21:44:55	2021-12-13 21:54:55	E.

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】**。

	000		(R) 8535	<b>Q</b> 816	() (10)	<b>র</b> গর	● 网络	Q Rin			讷	Rugarn 🔀 🗄	admin 🔫 C	200
母肪	服务器编策略													
2 健康检测	🕀 BERRE 🗋 SUM 🗙 HURK	新建服务器端策略										输入要查询的信息	Q豊富(	🔒 商級書
◎ 💄 用户	策略名称	策略名称								*(1-31:00F)		g:/+		9948
应用安全		DENHE	ssivpn											
◎ 小 对象组		PKUg	sslvpn							r				
I ACL		SSL协议版本①	Z SSL 3.0		Z TLS 1.0		🗹 TLS 1.1	1	V TLS 1.2	回出1.1				
0 🛙 SSI		加密會件	<ul><li>全部</li></ul>		中級	高级	0	国忠	○ 自定义					
skier posto Hinds			Q筛选				Q筛选							
2000年8月			可透				已透(2)							
- THE SECOND			SSL_RSA_w	ith_DES_CBC	_SHA	^	SSL_RSA_with	AES_128_CB	C_SHA					
· monecestim			SSL_RSA_W	ith RC4 128	SHA		SSL_KSA_WIT	1_AES_250_CB	C_SHA					
◎ ≪ 公销管理			SSL_RSA_w	ith_3DES_ED	E_CBC_SHA									
🐨 🐴 PKI			SSL_RSA_ed	coort_with_R	C4_40_MD5 C2_CBC_40_MD5									
・証书			SSL_RSA_et	port_with_D	ES_CBC_SHA									
<ul> <li>证书访问控制策略</li> </ul>			SSL_DHE_R	SA_with_AES	256 CRC SHA									
· 证书主题			SSL_RSA_A	ES_128_CBC	SHA256									
			SSL_RSA_A	ES_256_CBC SA_AES_128	SHA256 CRC SHA256									
		最大缓存会话数目	500		_000_000.000	*				( 100-20480 , BAND 500 )				
		会沃缓存期时时间								R (1-4294967295, MRB/5360	0)			
		验证就中国①	3000						-					
		united and the C	○关闭		● 升	<b>」</b> 届		○ 不强制	腰床					
	(m) ← (動) 0 页, 共					後定	1004							设有政策
			Сору	right© 200	4-2020 新华三	技术有限的	3司 版权所有	,保留一切权	利		_			

- 0 • ۲ HBC SecPath vFW100 ^ ⊕ 新建 🗙 删除 ⊙ 启用 🚫 禁用 📿 刷新 💘 VRF ◎□接口 网关 工作状态 IP地址 0.0.0.0 HTTPS编口 🛡 安全域 🔽 gw ● 生效 4443 ◎ 🖋 链路 编辑网关 DNS ARP 网关⑦ gw \*(1-31字符) MD IP地址⑦ IPv4 O IPv6 🖲 🍋 VPN 0.0.0.0 (缺省为0.0.0.0) 🔍 📉 SSL VPN HTTPS端口⑦ 访问实例
   网关
   · 客户端地址池 4443 (1025-65535,缺省为443) 开启HTTP流量重定 向 HTTP端口の (1025-65535,缺省为80) ・IP接入接口 SSL服务器端策略 sslvpn ·全局配置 VRF ·模板管理 公网 ¥ ·统计信息 便能 ~ ◎会路由 ◎组播 确定 取消 ◎ DHCP |← ← | 第 1 页,共1页 | → → | 毎页显示余数 25・ ◎ 🌷 服务 Copyright© 2004-2020 新华三技术有限公司 版权所有,保留一切权利
- 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

HBC SecPath vFW			<b>2</b>				<b>9</b>		
导航	↓ 访问实例	194.945	and at	- AK#0	-9 59K				
₩ VRF	🕀 ANTRE 🗙 HERRA 📿 REANT	编辑访问实例						@~	
◎□接口	✓ 访问实例名称		Nebulas T(	Pules IPul	es BVC	DVI/45 (\$2877	रना अध्यक्ष	THERE R	.F
🔋 安全域	context	on the		1 46.00		olation octation		^ X	网
◎ 🖋 链路		访问实例⑦	context		* (1-3	31字符)			
DNS		关联网关	🕀 新建 🕜	编辑 🗙 删除					
ARP 🖾			网关	访问方式	域	主机名称	(A) SHE		
MD			gw	直接访问网乡	ŧ		Ø		
🖲 🍋 VPN									
🖲 强 SSL VPN		VRF	公网		Ŧ				
访问实例		ISPikiEttt			Ŧ				
· 网关		开启给证明检证例							
· 客户端地址池		THERE AND A		-					
・IP接入接口		THEFT							
<ul> <li>・全局配置</li> </ul>		THESHALL		_/ <u>:</u> #_6	+				
・模板管理		THE REPORT OF TH	<ul> <li>Index (K276)</li> </ul>	01126 1	r				
·统计信息		THEIWCALLENGE							
◎ 🛞 路由		最大用户数	1048575	完成	(1-1) EV:36	,48575)		v	
◎♂组播				, 500					
🖲 🧇 DHCP	K ←   m   m + 1 m   -								
◎ 🍣 服务	, <u></u> , <u>,</u> <u>,</u> <u>,</u> <u>,</u> <u>,</u> <u>,</u> <u>,</u> <u>,</u> <u>,</u>	**************************************							
		Comut	iaht@ 2004 3	020 9546=14-	日本日八日	READ READ			

<sup>12,</sup> 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。



#### $\times$ 常规 🏹 选择证书 × 连接名 SSL VPN连接 🗌 运行后自动认证 颁发给 预期目的 颁发者 截止时间 🗌 使用短信验证码 WIN-OHN2GDK... 服务器端验证 2021-12-13 21:54:55 认证类型 Local • WIN-OHN2GDK... 客户端验证 • 认证模式 密码+证书认证 选择客户端证书... 确定 取消 确定取消



DM 12,7048       1.6.8.23       TP       66       252.44.9       -0.81 (R), ACI (Sec 20.4, 2000)         DM 12,7048       1.6.8.23       TP       6       252.44.9       -0.81 (R), ACI (Sec 20.4, 2000)         DM 12,7048       1.6.8.1       TP       5.9       243.41 (D)       1.9       5.9         DM 12,7048       1.6.8.1       1.6.8.23       TUS       5.9       2.9       2.9         DM 12,7048       1.6.8.1       1.6.8.23       TUS       5.9       2.9       2.9         DM 12,7048       1.6.8.1       1.6.8.23       TUS       7.9       7.9       7.9         DM 12,7048       1.6.8.1       1.6.8.23       TUS       7.9       7.9       7.9         DM 12,7048       1.6.8.23       TUS       1.8       7.9       7.9       7.9         DM 12,7048       1.6.8.23       TUS       1.8       7.9       7.9       7.9       7.9         DM 12,7048       1.6.8.23       TUS       7.9	1793 12.734198	1.0.0.233	1.0.0.1	TCP	66	128 4863 + 4443 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=8960 WS=256 SACK_PERM=1
1976 [17:46]       1.6.8.13       1.6.8.1       100       54       124 400 = 440 [1613 test]. Auch Links/250 Linke         1976 [17:46]       1.6.8.1       1.6.8.1       100       54       235 kerne high         1978 [17:391       1.6.8.1       1.6.8.23       100.4       134       235 kerne high         1978 [17:391       1.6.8.1       1.6.8.23       100.4       235 kerne high       235 kerne high         1978 [17:391       1.6.8.1       1.6.8.23       100.4       235 kerne high       235 kerne high         1978 [17:391       1.6.8.1       1.6.8.23       10.4       1364       235 kerne high         1978 [17:391       1.6.8.1       1.6.8.23       10.4       1364       235 kerne high         188 [17:492       1.6.8.23       1.6.4       10.4       236       236 kerne high       236 kerne high         188 [17:492       1.6.8.23       1.6.4       10.4       236       236 kerne high       366 kerne high       376 kern	1794 12.734438	1.0.0.1	1.0.0.233	TCP	66	255 4443 - 4063 [SYN, ACK] Seq+0 Ack=1 Win+65535 Len+0 MSS=1460 SACK_PERM+1 NS=1
198 B 27827 1.4.8.33 1.4.8.4 1.1054 1.23 1.136 1.137 1.136 1.137 1	1795 12.734461	1.0.0.233	1.0.0.1	TCP	54	128 4063 = 4443 [ACK] Seq=1 Ack=1 Win=525568 Len=0
127 12.7393 1.6.8.1 1.8.8.23 10.51 1354 25 Serve Hills 127 12.7393 1.6.8.1 1.8.8.23 10.51 137 47 25 Serve Hills 128 12.7393 1.6.8.1 1.8.8.23 10.51 137 47 25 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.3 1.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7393 1.6.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7493 1.6.8.1 1.8.1 1.9.1 128 55 Serve Hills 128 12.7493 1.6.8.1 128 55 Serve Hills 128 12.7493 1.6.8.1 128 55 Serve Hills 128 12.7493 1.6.8.1 128 55 Serve Hills 1.9.1 128 55 Serve	1796 12.734527	1.0.0.233	1.0.0.1	TLSv1	253	128 Client Hello
198 B.27081 1.6.8.1 1.6.8.20 1.0.1 1.0.4.20 1.0.1 1.0.1 07 20 Confliction, Confliction Str., Period Phile Deer 198 B.27081 1.6.8.1 1.6.8.2 1.0.1 1.0.	1797 12.734763	1.0.0.1	1.0.0.233	TLSv1	1514	255 Server Hello
12012 17:001         1.0.0.13         1.0.0.1         102         120 001 -0.001 (c) 0000 (c) 00000 (c) 0000 (c) 0000 (c) 0000 (c) 00000 (c) 0000 (c) 0000 (c) 0	1798 12.739343	1.0.0.1	1.0.0.233	TLSv1	497	255 Certificate, Certificate Request, Server Hello Done
1888 12.74034       1.6.8.1<	1799 12.739370	1.0.0.233	1.0.0.1	TCP	54	128 4863 + 4443 [ACK] Seq=200 Ack=1984 Win=525568 Len=0
Statistics and Statistics (Statistics (	1880 12.742138	1.0.0.233	1.0.0.1	TLSv1	2185	128 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
180 12.2027 1.4.2.3 1.4.2.1 1.51 2.6 124 picture bran, splitzette bran 180 12.2027 1.4.2.3 1.4.2.3 1.4.2.1 1.51 2.6 124 picture bran, splitzette bran 180 12.2027 1.4.2.3 1.	1881 12.745814	1.0.0.1	1.0.0.233	TLSv1	1288	255 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
<pre>see 180: 215 bytes on size (1248 bits), 215 bytes captured (1248 bits) on inter-face WardsWF (12480464-956-9564-956-9564-956-9564-956-9564-956-9564-956-9564-956-9564-956-9564-956-9564-956-9564-956-9564-956-9564-956-9564-956-9564-956-9564-956-9564-956-9564-956-956-956-956-956-956-956-956-956-956</pre>	1882 12.745277	1.0.0.233	1.0.0.1	TLSv1	256	128 Application Data, Application Data
ene 118: 118 types on une (2008 110), 218 types captured (2008 111) in iterates (backs/97 (2018/06-9762-9056-9762-9056-9762-9056-9762-9056-9762-9056-9762-9056-9762-9056-9762-9056-9766-9762-9056-9766-9766-9766-9766-9766-9766-9766-97						
<pre>% Tisk need Lyne: Needbalk Protocol: Gertificate Genes Type Section (Type Section</pre>	Transmission Contr Transport Layer Se	ol Protocol, Src P curity	ort: 4063, Dst Port:	4443, Seq: 20	90, Ack: 19	04, Len: 2131
Context Type: Readballs Leggt: 190 * Readballs Protocol: Certificate Section 200 * Readballs Protocol: Certificate Section 200 * Readballs Protocol: Certificate Section 200 * Certificate Leggt: 190 * Certificate Leggt	Y TLSv1 Record La	ver: Handshake Pro	tocol: Centificate			
<pre>write::::::::::::::::::::::::::::::::::::</pre>	Content Type	Handshake (22)				
length: JBS insolate frequencies insolate	Version: TLS	1.0 (0x0301)				
* Restinges Protocil (etiting) (etiting) (etitions) (etiting) (etitions) (etiting) (etitions) (e	Length: 1789					
Register Type: Gertflicter (D12 Syte) Certflicter (D12 Syte) SUBJURGENTERSUBJURGENDERSDERSDERSDERSDERSDERSDERSDERSDERSDERS	<ul> <li>Handshake Pro</li> </ul>	stocol: Centificat				
Certificate length: DB Certificate length: SB Certificate length: SB Certif	Handshake	Type: Certificate	(11)			
Generalizations (172) [pixs]	Length: 1	85				
Continues Length: Bit Continues Length: B	Cercificat	es congen: 1762				
<ul> <li>Certificate: 388/2014/2020/2014/2020/2014/2020/2014/2014</li></ul>	<ul> <li>Carcitical</li> </ul>	ws (1762 Dytws)				
Generations largels 79 Certificate largels 79 Total faces (Largels 79	Cantilia Cantilia	ante Lengen. 501	0360-0020301030312540	0000001745461	the falses i	A second descent and the complement of a second descent blackborrer is a second above the test of the test of the second
i curtificate: 30801/190801/40900000000000000044cr6455. (L6-at-comentane-4016-04000000p-G3) TSA Record Layer: Inaddabas Petetocial LeftHicate Verfy TSA Record Layer: Inaddabas Petetocial LeftHicate Verfy TSA Record Layer: Inaddabas Petetocial: Encryption Handabas Records TSG4 Record Layer: Inaddabas Petetocial: Encryption Handabas Records	Cartifi	cate Length: 795	02030003020102021334	00000071340.	no- (hees-	a a construction and a construction of the second
Tubbi Record Layer: Handhakk Protocol: Encrysted Headhakk Message Tubbi Record Layer: Compt Captor See Protocol: Encrysted Headhakk Message	) Cantifs	cate: 381283173813	0166-001020102021056	057426442679	45 (14.44	- COMPANY AND A CONTRACTOR AND A
Tubli Rocci Layer: Nanchaka Protocal: LevelTikera Worty Tubli Rocci Uguer: Amerikan Protocal: Tuber Tiper Spec Tubli Rocci Uguer: Nanchaka Protocal: Encrysted Handhaka Rossage	TISUL Record La	on: Handrhake Roo	torol: Client Key Exc	handa	1401 (10-0C	comornane, nasi o nacionego eny
TLSGE Record Layer: Onling Cipher Sea: Protocoll: Design Cipher Spec TLSGE Record Layer: Handhake Protocoll: Encrypted Heshake Message	TLSv1 Record La	ven: Handshake Pro	torol: Centificate Ve	elfy		
) TLS/L Record Layer: Handshake Protocal: Encrypted Handshake Message	TISv1 Record La	er: Change Cinher	Ster Protocol: Chang	e Cinhen Sner		
	TI Svd. Record La	en: Handshake Pro	torol: Encrypted Hand	shake Message		

以上,使用SSL VPN证书双向认证已顺利完成!

无

配置关键点