配置ASA作为本地CA服务器和AnyConnect数据 转发器

Contents

Introduction **Prerequisites** Requirements **Components Used** 背景信息 Configure **Network Diagram** ASA作为本地CA服务器 步骤1.配置和enable (event)在ASA的本地CA服务器 步骤2.创建并且添加用户到ASA数据库 步骤3.在广域网接口的Enable (event) WebVPN 步骤4.导入在客户端机器的认证 ASA作为AnyConnect客户端的一个SSL网关 ASDM AnyConnect配置向导 配置AnyConnect的CLI Verifv Troubleshoot **Related Information**

Introduction

本文描述如何设置Cisco可适应的安全工具(ASA)作为Certificate Authority (CA)服务器和作为Cisco AnyConnect安全移动客户端的安全套接字协议层(SSL)网关。

Prerequisites

Requirements

Cisco 建议您了解以下主题:

- •运行软件版本9.1.x的基本的ASA配置
- ASDM 7.3或更高

Components Used

本文档中的信息基于以下软件和硬件版本:

- •运行软件版本9.1(6)的Cisco 5500系列ASA
- AnyConnect Windows的安全移动性客户端版本4.x

- •运行支持的OS每张<u>兼容性图的</u>PC。
- Cisco Adaptive Security Device Manager (ASDM)版本7.3

Note:请从 <u>Cisco 软件下载</u>中下载 AnyConnect VPN Client 程序包 (anyconnect-win*.pkg) (仅限<u>注册用户</u>)。将 AnyConnect VPN Client 复制到 ASA 的闪存中以供远程用户计算机下载 ,以便建立与 ASA 的 SSL VPN 连接。有关 ASA 配置指南的详细信息,请参阅<u>安装</u> <u>AnyConnect 客户端</u>部分。

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

背景信息

在ASA的认证机关提供这些功能:

- •集成在ASA的基本的认证机关操作。
- 配置证书。
- •提供安全撤销检查发出的认证。
- 在ASA提供认证机关为了用在浏览器based(WebVPN)和客户端based(AnyConnect) SSL VPN连接上。
- •提供委托数字证书给用户,不用需要取决于外部验证授权。
- •为证书验证提供一个安全,机构内部的权限和提供直接的用户登记通过网站登录。

指南和限制

- 支持在路由的和透明防火墙模式下。
- 仅一个本地CA服务器可以每次是常驻在ASA。
- •作为本地CA服务功能故障切换设置不支持ASA。
- •作为本地CA服务器的ASA只到现在支持SHA1证书的生成。
- •本地CA服务器可以用于基于浏览器的和基于客户的SSL VPN连接。目前不支持为IPSec。
- 不支持本地CA的VPN负载均衡。
- •本地CA不可以是辅助到另一个CA。它能仅作为根CA。
- •目前ASA不能登记到本地CA身份认证的服务器。
- 当证书登记完成时,ASA存储包含用户的密钥对和证书链的一个PKCS12文件,要求大约闪存 或磁盘空间2 KB每个登记。实际金额磁盘空间取决于被配置的RSA密钥大小和认证字段。请记 住此指南,当添加在ASA的很大数量的待定证书登记与有限的可用闪存时,因为这些 PKCS12文件在被配置的登记检索超时的期限的闪存存储。

Configure

此部分描述如何配置Cisco ASA作为本地CA服务器。

Note:使用<u>命令查找工具</u>(<u>仅限注册用户</u>)可获取有关本部分所使用命令的详细信息。

Network Diagram



Client machine with AnyConnect ASA Configured as a Local CA server and AnyConnect Headend

ASA作为本地CA服务器

步骤1.配置和enable (event)在ASA的本地CA服务器

- 连接对Configuration>远程访问VPN > Certificate Management >本地认证机关> CA服务器。检查Enable (event)认证机关服务器选项。
- 配置密码短语。密码短语应该是用于编码和保存PKCS12文件包括本地CA证书和密匙对的最小数量,7个字符。如果CA证书或密钥对丢失,密码短语打开PKCS12档案。
- •配置发证者名字。此字段将出现作为根证明CN。这在以下格式可以指定:CN (普通的名字), OU (组织单元), (o)组织、L (现场), S (状态)和C (国家)。
- •可选配置:配置SMTP服务器,并且保证OTP的电子邮件服务器设置可能被接受通过邮件结束 客户端完成登记。您可以配置您的本地Email/SMTP服务器的主机名-或IP地址。您可以从地址 和客户端会收到电子邮件的主题领域也配置。默认情况下,从地址是admin@<ASA主机名->.null和主题是证书登记邀请。
- 可选配置: 您可以配置可选参数类似客户端密钥大小, CA服务器密钥大小、CA证书寿命和客 户端证书寿命。

 Add Delete S Connect Configure the Local Certificate Authority. To make configuration changes after it has been configured for the first time, disable the Local Certificate Authority. Configure the Local Certificate Authority. To make configuration changes after it has been configured for the first time, disable the Local Certificate Authority. Configure the Local Certificate Authority. To make configuration changes after it has been configured for the first time, disable the Local Certificate Authority. Configure the Local Certificate Authority. To make configuration changes after it has been configured for the first time, disable the Local Certificate Authority. Configure the Local Certificate Authority. To make configuration changes after it has been configured for the first time, disable the Local Certificate Authority. Configure the Local Certificate Authority. To make configuration changes after it has been configured for the first time, disable the Local Certificate Authority. Configure the Local Certificate Authority. To make configuration changes after it has been configured for the first time, disable the Local Certificate Authority. Configure the Local Certificate Authority Server Enable the option to make ASA as Local CA Passphrase: Configure the Local Certificate Authority. Configure the Local Certificate Buthority. Configure the Local Certificate Buthority. Configure the Local Certificate Buthority. Contender SSL VPN Access Configure the Local Certif	Device List 🗇 🖗	×	Configuration > Remote Access VPN	> Certificate Management > Local Certificate Authority > CA Server
Ind: Co Control Control Passphrase: Confirm Passphrase: Issuer Name: Confirm Passphrase: Specify the Passphrase Issuer Name: CA Server Key Size: Specify the Server/Client key-size to Clent Key Size: Specify the Server/Server Clent Certificate Lifetime: Streer Name Streer Name/IP Address: From Address: Server Name/IP Address: From Address: Subject: Certificate Streer More Options	🕈 Add î Delete 🚿 Connect		Configure the Local Certificate Authority	7. To make configuration changes after it has been configured for the first time, disable the Local Certificate Authority.
ID.105.130.6924443 Passphrase: Confirm Passphrase: ID.20105.130.6924443 Passphrase: Confirm Passphrase: ID.20105.130.6924443 Passphrase: Confirm Passphrase: ID.20105.130.6924443 Passphrase: ID.20105.130.6924445	Find: Go		Enable Certificate Authority Server	Enable the option to make ASA as Local CA
Passphrase:				
Confirm Passphrase: Specify the Passphrase Issuer Name: CN=ASA.local CA Server Key Size: J024 Clent Key Size: J024 Clent Key Size: J024 CA Certificate Lifetime: 1095 CA Certificate Lifetime: 1095 Introduction Clent Certificate Lifetime: Network (Clent) Access Server Xey Size: Chentess SSI, VPN Access Server Name/IP Address: AAAL/Local Users Server Name/IP Address: From Address: admin@cliscoasa.null Subject: Certificate Enrolment Invitation More Options More Options			Passphrase:	
Issuer Name: CN=ASA.local Specify the CN which will show as Issuer name CA Server Key Size: 1024 Specify the Server/Client key-size to be used Clent Key Size: 1024 Specify the Server/Client key-size to be used CA Certificate Lifetime: 1095 days Throduction Throduction ShTP Server & Email Settings Secure Desktop Manager Server Name/IP Address: From Address: Host Scan Image Subject: Certificate Enrolment Invitation More Options More Options More Options			Confirm Passphrase:	Specify the Passphrase
CA Server Key Size: Clent Key Size: Clent Key Size: CA Certificate Lifetime: Network (Clent) Access Clent Certificate Lifetime: Network (Clent) Access Clent Certificate Lifetime: Network (Clent) Access Clent Certificate Lifetime: AAAAL/Accel Users AAAAL/Accel Users AAAAL/Cart Users AAAAL/Car			Issuer Name:	CN=ASA.local Specify the CN which will show as Issuer nam
Client Key Size: CA Certificate Lifetime: Client Certificate Lifetime: SMTP Server & Email Settings Server Name/IP Address: From Address: Certificate Management Ca Certificates Ca Certificates Ca Certificate Solution More Options More Options			CA Server Key Size:	1024 👻
CA Certificate Lifetime: 1095 days Introduction Introduction 365 days Introduction SMTP Server & Email Settings AAAA,Local Users Server Name/IP Address: AAAA,Local Users From Address: From Address: Server Name/IP Address: Secure Desktop Manager Subject: Ca Certificate Management Subject: Ca Certificate Signer Certificate Authority			Client Key Size:	1024 Specify the Server/Client key-size to
Remote Access VPN Introduction Introduction Network (Client) Access Client Certificate Lifetime: 365 days SMTP Server & Email Settings Server Name/IP Address: From Address: From Address: Certificate Management Certificate Management Cartificate Signer Code Signer Code Signer Code Signer Code Signer Code Signer Code Cificate Authority More Options			CA Certificate Lifetime:	1095 days
Remote Access VPN Introduction Introduction Network (Client) Access Client Certificate Lifetime: 365 days SMTP Server & Email Settings SMTP Server & Email Settings SMTP Server & Email Settings SMTP Server Name/IP Address: AAA/Local Users Host Scan Image Certificate Management Certificates Cartificates Identity Certificates Introduction Code Signer Local Certificate Authority More Options				The CA certificate lifetime change will take effect after existing CA certs expire.
Introduction Hetwork (Client) Access Clientiess SSL VPN Access AAA/Local Users AAA/Local Users From Address: AAA/Local Users From Address: Addicts Subject: Certificate Management Subject: Certificates Accertificates Accertificate Pool Code Signer Code Signer Code Certificate Authority	Remote Access VPN	џ	Client Certificate Lifetime:	365 days
Image: Support of the stress of the stres	····· 🦓 Introduction			
Image: Certificate Management Server Name/IP Address: Image: Certificate Management From Address: Image: Certificate Management Subject: Image: Certificate Management Subject: Image: Certificate Management More Options	Network (Client) Access	- 1	SMTP Server & Email Settings	
AAA,Local Users From Address: admin@ciscoasa.null Aspectary Subject: Certificate Enrollment Invitation Cortificates More Options Trusted Certificate Pool More Options Cocal Certificate Authority Certificate Authority	Clientless SSL VPN Access	- 1	Server Name/IP Address:	
Barnet Scall integer From Redictor Image: Control Desktop Manager Subject: Image: Control Desktop Manager More Options	AAA/Local Users	- 1	From Address:	admin@ciscoasa.null
Image: Control of this state Subject: Image: Control of this state Subject: Image: Control of this state More Options		- 1	n on Plaa cast	
Accertificates More Options Accertificates More Options Accertificate Pool Accertificate Pool Accertificate Authority Acceltificate Authority	Certificate Management	- 1	Subject:	Certificate Enrollment Invitation
Identity Certificates More Options Image: Application of the second of		- 1		
- 20 Trusted Certificate Pool - 20 Code Signer - 20 Local Certificate Authority		- 1	More Options	
- 2 Code Signer - B Local Certificate Authority	- 2 Trusted Certificate Pool	- 1		
Eg Local Certificate Authority		- 1		
	Local Certificate Authority	- 1		
	CA Server	- 1		
Wanane leer Certificates	Manage User Database			
	: Englishinge oder Geründsteb			

等效的 CLI 命令:

ASA(config)# crypto ca server ASA(config-ca-server)# issuer-name CN=ASA.local ASA(config-ca-server)# subject-name-default CN=ASA.local ASA(config-ca-server)# lifetime certificate 365 ASA(config-ca-server)# lifetime ca-certificate 1095 ASA(config-ca-server)# passphrase cisco123 ASA(config-ca-server)# no shutdown % Some server settings cannot be changed after CA certificate generation. Keypair generation process begin. Please wait...

Completed generation of the certificate and keypair...

Archiving certificate and keypair to storage... Complete

这些是可能被配置在本地CA服务器配置下的另外的字段。

协制스피占니미	这是ASA的CRL位置。
在前力 能 点 U R L	默认位置是 <u>http://hostname.domain/+CSCOCA+/asa_ca.crl,</u> 但是可能修改URL。
ᄮᆂᇬᆈᅓᇦᇷᄤᆿ	要使CRL可以HTTP下载在一个指定接口和端口,从下拉列表请选择发布CRL接口。然
反 甲 U R L 按 L 和 峏 L	默认的端口号是TCP端口80。
CDI 丰仝	本地CA更新并且补发CRL,在用户证书被取消或未撤回时候,但是,如果没有撤销更
UKL对叩	寿命crlcommand指定在本地CA配置时的时期。如果不指定CRL寿命,默认时间是六
粉 捉 医 友 禄 位 罟	使用本地CA数据库, ASA访问并且实现用户信息、发出的认证和撤消清单。默认情况
奴加汗行间 区區	一个外部文件系统 驻留 或者可以被配置驻留。
	输入默认主题(DN字符串)添附到在发出的认证的用户名。允许的DN属性在此列表提供
	• CN (普通的名字) SN (姓氏)
	• O (组织名字)
	• L (现场)
默认主题名称	• C (国家)
	• OU (组织单位)
	• EA (电子邮件地址)
	• ST (州/省)
	• T (标题)
登记期间	以内用户可能从ASA检索PKCS12文件的几小时定登记时间限制在。

DEFAULT值是24小时。

Note:如果登记期间到期,在用户检索包括用户证书的PKCS12文件前,登记没有允许。 一次密码到期 以几小时定义了时间OTP为用户登记是有效的。当用户允许登记时,此时间开始。de 证书到期提示 指定几天的数量,在认证到期前重新登记一个最初的提示被发送到认证责任人。

步骤2.创建并且添加用户到ASA数据库

 连接对Configuration>远程访问VPN > Certificate Management >本地认证机关>管理 Database.Click添加的用户。

Device List	Ψ ^ _	onfiguration > Remote Access	s vPN > Certificate Manag	ement > Local Certifica	<u>te Authority</u> > <u>Manage User Database</u>	2	
🕈 Add 🃋 Delete 🚿 Connect		Manage the users in the user datab	base for Local Certificate Aut	hority Server.			
nd: Go		Username	Emai		Subject Name		Add
							Edit
							Delete
							Allow Enrollment
							Email OTP
							View/Re-generate OTP
Remote Access VPN	07 P						
? Introduction							
Network (Client) Access							
Clientless SSL VPN Access							
Host Scap Image							
E Secure Desktop Manager							
Certificate Management							
- 2 CA Certificates							
- 🚰 Identity Certificates							
- 2 Trusted Certificate Pool							
E Local Certificate Authority							
Manage User Database							

•如此镜像所显示,即指定用户选派用户名、电子邮件ID和主题名称。

🔁 Add User		×				
Username:	user 1					
Email ID:	user1@cisco.com					
Subject (DN String):	CN=user1,OU=TAC Select					
Allow enrollment						
(Add User Cancel Help					

•保证**允许登记**被检查,以便您允许为认证登记。

•点击**添加用户时**完成用户配置。

等效的 CLI 命令:

ASA(config)# crypto ca server user-db add user1 dn CN=user1,OU=TAC email user1@cisco.com • 在用户被添加到用户数据库后,登记状态显示如**准许登记**。

Configura	ation > Remote Access VPN >	Certificate Management > Local	Certificate Authority > <u>Manage User Dat</u>	abase		
Manage	the users in the user database for	Local Certificate Authority Server.				
Userna	me	Email	Subject Name	Enrollment Status	Certificate Holder	Add
user 1		user1@cisco.com	CN=user1,OU=TAC	allowed	yes	Edit
						Delete
						Allow Enrollment
						Email OTP
						View/Re-generate OTP
					I	

验证用户状态的CLI :

ASA# show crypto ca server user-db

username:	userl					
email:	user10cis	sco.d	com			
dn:	CN=user1,	, OU=1	ГАС			
allowed:	19:03:11	UTC	Thu	Jan	14	2016
notified:	1 times					

- enrollment status: Allowed to Enroll
 - 在用户被添加了到用户数据库后,一个次密码(OTP),用户的能完成登记,可以提供使用二者 之一这:

给OTP发电子邮件(要求SMTP服务器和电子邮件设置将被配置在CA服务器配置下)。

或者

请直接地查看OTP,并且与用户的共用通过点击View/Re生成OTP。这可能也用于regenrate OTP。



等效的 CLI 命令:

ASA# show crypto ca server user-db username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: 19:03:11 UTC Thu Jan 14 2016 notified: 1 times enrollment status: Allowed to Enroll

步骤3.在广域网接口的Enable (event) WebVPN

•在ASA的Enable (event) Web访问客户端的能请求为登记。

ASA# show crypto ca server user-db username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: 19:03:11 UTC Thu Jan 14 2016 notified: 1 times enrollment status: Allowed to Enroll

步骤4.导入在客户端机器的认证

- •在客户端工作站请打开浏览器并且连接对链路为了完成登记。
- •用于此链路的IP/FQDN应该是WebVPN在该步骤被启用,是接口互联网接口的IP。

https://<ASA IP/FQDN>/+CSCOCA+/enroll.html

• 输入用户名(配置在ASA在第2步,选项A)和**OTP下,**通过**电子邮件**提供或**手工**。

Certificate	Attps://10.105.130.69/-	CSCOCA+/login.html	🔎 👻 😋 Certificate error 🖒	<i> 10.105.130.69</i>	×
ili. cisi	as co	A - Local Certificate Authority			
ASA	A - Local Certificate Auth	ority			
Username	user1				
One-time Pa	assword		Enter the User-Name and 0	OTP provided	
	Submit Reset				
NOTE: On succ	essful authentication:				
Open or Install the Close all Restart t	Save the generated ce e certificate in the brow the browser windows, he SSL VPN connection	rtificate ser store and n			
•点击开放ī	直接地安装从A	SA接收的客户端证书			
 安装客户如 		语同一样OTP接受前	。 ī的。		
File Down	oad				X
Do you	want to op	pen or save this	s file?		
	Name:	user1.p12			
	Type:	Personal Inform	nation Exchange		
	From:	10.105.130.214			
		Open	Save	Canc	el
2	While files f harm your c save this file	rom the Internet ca omputer. If you do e. <u>What's the risk?</u>	an be useful, some not trust the sourc	files can pote e, do not ope	entially en or

Certificate Import Wizard



x

• 留下路径作为默认值并且**其次**点击。

Certificate Import Wizard	x
File to Import Specify the file you want to import.	
File name: s\Temporary Internet Files\Content.IE5\SQT1AUGH\user1[1].p12 Browse	
Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX,.P12)	
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B) Microsoft Serialized Certificate Store (.SST)	
Learn more about <u>certificate file formats</u>	
< Back Next > Cancel	

- 送进OTP在密码字段。
- •您能选择选项**指示此键如可输出,**以便键能从工作站如果必须被导出今后。
- **其次**点击

Certificate Import Wizard
Password To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
••••••
 Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option. Mark this key as exportable. This will allow you to back up or transport your keys at a later time. Include all extended properties.
Learn more about protecting private keys
< Back Next > Cancel

- •您能在一特定的证书存储上手工安装认证或留下它自动地选择存储。
- 单击 Next。

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse
Learn more about certificate stores
< Back Next > Cancel

•点击**完成**为了完成安装。

Certificate Import Wizard



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:







• 一旦成功安装认证,您能验证它。

•打开IE并且连接对工具> Internet选项。



•如此镜像所显示,连接**使**选项满意并且点击**证书**。

Internet Options							
General Security Privacy Content Connections Programs Advanced							
Parental Controls Control the Internet content that can Parental Controls be viewed.							
Content Advisor Ratings help you control the Internet content that can be viewed on this computer. Enable Settings							
Certificates Use certificates for encrypted connections and identification.							
Clear SSL state Certificates Publishers							
AutoComplete							
AutoComplete stores previous entries Settings on webpages and suggests matches for you.							
Feeds and Web Slices							
Feeds and Web Slices provide updated Settings content from websites that can be read in Internet Explorer and other programs.							
OK Cancel Apply							

• 在私有存储下,您能看到从ASA接收的认证。

Certificates					x
Intended purp	oose: <a< th=""><th> ></th><th></th><th></th><th>•</th></a<>	>			•
Personal C	ther People	Intermediate Certification /	Authorities T	rusted Root Certification 4	
Issued To		Issued By	Expiratio	Friendly Name	
🔄 user 1		asa.local	1/8/2017	ou=TAC,cn=user1	
Import	Evport	Bemove		Advance	
Certificate ir	ntended purpo	ses			
Learn more a	bout <u>certificat</u>	<u>es</u>		View	
Import Certificate in	Export.	Remove		View	

ASA作为AnyConnect客户端的SSL网关

ASDM AnyConnect配置向导

AnyConnect配置Wizard/CLI可以用于为了配置AnyConnect安全移动性客户端。保证AnyConnect客 户端程序包被加载了到ASA防火墙的闪存/磁盘,在您进行前。

完成这些步骤为了通过配置向导配置AnyConnect安全移动性客户端:

1. 日志到ASDM里和连接到启动配置向导的Wizards> VPN向导> AnyConnect VPN向导并且其次 点击。

TanyConnect VPN Connecti	on Setup Wizard	23
VPN Wizard	Introduction	
	protected using either the IPsec or the SSL protocol. The ASA will automatically upload the AnyConnect VPN Client to the user's device when a VPN connection is established.	end
Corporate	VPN Remote Access	
Network		
[< Back Next > Cancel H	elp

2. 输入连接配置文件名字,选择VPN从VPN访问接口下拉菜单将被终止的接口,并且其次点击。

The AnyConnect VPN Connection Setup Wizard			
Steps 1. Introduction	Connection Profile Identification This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections.		
2. Connection Profile Identification 3. VPN Protocols	Connection Profile Name: SSL_GRP		
 Client Images Authentication Methods Client Address Assignme 	VPN Access Interface: Internet		
 Network Name Resolutio Servers NAT Exempt 			
9. AnyConnect Client Deployment 10. Summary			
	< Back Next > Cancel Help		

3. 检查**SSL**复选框为了enable (event)安全套接字协议层(SSL)。设备认证可以是一个委托的第三方 Certificate Authority (CA)发出的认证(例如Verisign或者Entrust),或者自签证书。如果认证在ASA上 已经安装,则可以通过下拉菜单被选择。

1. **Note**:此认证是将由ASA提交给SSL客户端的服务器端认证。如果比必须生成没有在ASA上当 前安装的服务器证明自签证书,则请点击**管理**。为了安装一个第三方认证,请完成在<u>ASA</u>

8.x描述<u>手工安装第三方供应商证书为了用在WebVPN配置示例</u>Cisco文档上的步骤。Enable

X

(event) VPN协议和设备认证。单击 Next。

AnyConnect VPN Connection Setup Wizard

Steps	VPN Protocols
 Steps Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods Client Address Assignme Network Name Resolutio Servers NAT Exempt AnyConnect Client Deployment Summary 	VPN Protocols AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support. SSL IPsec Device Certificate Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA. Device Certificate:
	< Back Next > Cancel Help

4. 点击添加为了添加AnyConnect客户端程序包(.pkg文件)从本地驱动器或从ASA闪存/磁盘。

点击**访问闪存**为了从闪存驱动器添加镜像或者点击**加载**为了从主机本地驱动器添加镜像。

AnyConnect VPN Connect	ion Setup Wizard	22	
Steps	Client Images		
1. Introduction	ASA can automatically upload the latest AnyConnect package to the clien	nt device when it accesses the enterprise network.	
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to		
3. VPN Protocols	the top of the list.		
4. Client Images			
5. Authentication Methods			
6. Client Address Assignme	Image	Regular expression to match user-agent	
7. Network Name Resolutio Servers			
8. NAT Exempt			
9. AnyConnect Client Deployment			
10. Summary			
	You can download AnyConnect Client packages from <u>Cisco</u> by searching	'AnyConnect VPN Client' or <u>dick here</u> .	
< Back Next > Cancel Help			

- •您可能从ASA闪存加载AnyConnect.pkg文件/磁盘(如果程序包已经是那里)或从本地驱动器。
- •访问闪存--从ASA闪存/磁盘选择AnyConnect程序包。

- •加载-选择AnyConnect程序包从主机本地驱动器。
- •单击 Ok。

Add AnyConnect Client Image	23
AnyConnect Image: disk0:/anyconnect-win-4.2.00096-k9.pkg	Browse Flash
	Upload
Regular expression to match user-agent	×
OK Cancel Help	

• 单击 Next。

AnyConnect VPN Connect	tion Setup Wizard	×	
Steps	Client Images		
1. Introduction	ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network.		
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to		
3. VPN Protocols	the top of the list.		
4. Client Images			
5. Authentication Methods			
6. Client Address Assignme	Image	Regular expression to match user-agent	
 Network Name Resolutio Servers 	disk0:/anyconnect-win-4.2.00096-k9.pkg		
8. NAT Exempt			
 AnyConnect Client Deployment 			
10. Summary			
	You can download AnyConnect Client nackages from Cisco by searching	'AnyConnect VPN Client' or dick here	
Tou can download Anyconnect client packages from <u>Cisco</u> by searching Anyconnect vew client or <u>cick nere</u> .			
	< Back Next >	Cancel Help	

5. 用户认证可以通过验证、授权和统计(AAA)服务器组完成。如果已经配置用户,则请选择**本地并 且其次**点击。请添加一个用户到本地用户数据库并且**其次**点击。

Note:在本例中,配置本地认证,因此意味着在ASA的本地用户数据库将使用认证。

AnyConnect VPN Connect	tion Setup Wizard	23
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. Client Address Assignme 7. Network Name Resolutio Servers 8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary	Authentication Methods This step lets you specify the location of the authentication server. You can click on the "New" button to create a new server group. AAA Server Group: LOCAL New Local User Database Details Gisco User to be Added Username: user1 Add >> Delete Confirm Password: ••••• 	
	< Back Next > Cancel He	elp

6. 保证配置VPN客户端的地址池。如果那么已经配置得IP池请选择它从下拉菜单。否则,请点击**新** 为了配置。一旦完全,**其次请**点击。

AnyConnect VPN Connect	tion Setup Wizard
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. Client Address Assignment 7. Network Name Resolutio Servers 8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary	Client Address Assignment This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect. IPv6 address pool is only supported for SSL connection. IP v4 Address Pool IP v6 Address Pool Address Pool:Select New Details of the selected address pool
	< Back Next > Cancel Help

add IPv4 Pool	×
Name:	VPN_Pool
Starting IP Address:	10.10.10.1
Ending IP Address:	10.10.200
Subnet Mask:	255.255.255.0 👻
ОК	Cancel Help

• 单击 Next。

AnyConnect VPN Connect	tion Setup Wizard
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. Client Address Assignment 7. Network Name Resolutio Servers 8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary	Client Address Assignment This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect. IPv6 address pool is only supported for SSL connection. IP v4 Address Pool IP v6 Address Pool Address Pool VPN_Pool New Details of the selected address pool Starting IP Address: 10.10.10.200 Subnet Mask: 255.255.255.0 Vertice address Pool V
	< Back Next > Cancel Help

7. 随意地,请配置域名系统(DNS)服务器和Dns到DNS和域名字段,**其次**然后点击。

anyConnect VPN Connect	tion Setup Wizard
Steps	Network Name Resolution Servers
1. Introduction	This step lets you specify how domain names are resolved for the remote user when accessing the internal network.
2. Connection Profile Identification	DNS Servers:
3. VPN Protocols	WINS Servers:
 Client Images 	Domain Name:
5. Authentication Methods	
6. Client Address Assignme	
7. Network Name Resolution Servers	
8. NAT Exempt	
9. AnyConnect Client Deployment	
10. Summary	
	< Back Next > Cancel Help

8. 保证客户端和内部的子网之间的数据流一定是豁免从所有动态网络地址转换(NAT)。Enable (event)**从网络地址转换**复选框的**豁免VPN流量**和配置将使用免税的LAN接口。并且,请指定必须豁 免的本地网络并且**其次**点击。

anyConnect VPN Connec	tion Setup Wizard	X
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. Client Address Assignme 7. Network Name Resolutio Servers 8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary	NAT Exempt If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation. © Exempt VPN traffic from network address translation Inside Interface is the interface directly connected to your internal network. Inside Interface: Inside Local Network is the network address(es) of the internal network that client can access. Local Network: 192.168.10.0/24 The traffic between AnyConnect client and internal network will be exempt from network address translation.	
	< Back Next > Cancel He	lp 🛛

9. 单击 Next。

anyConnect VPN Connect	tion Setup Wizard	23
Steps	AnyConnect Client Deployment	
1. Introduction	AnyConnect client program can be installed to a client device by one of the following two methods:	
2. Connection Profile Identification	 Web launch - On accessing the ASA using a Web Browser, the AnyConnect client package will be automatically installed Pre-deployment - Manually install the AnyConnect client package. 	;
3. VPN Protocols		
Client Images		
5. Authentication Methods		
6. Client Address Assignme		
 Network Name Resolutio Servers 		
8. NAT Exempt		
9. AnyConnect Client Deployment		
10. Summary		
	< Back Next > Cancel He	lp

10. 最终步骤显示汇总,点击**完成**完成设置。

anyConnect VPN Connection Setup Wizard					
VPN Wizard	Summary				
Branch	Here is the summary of the configuration.				
EDIT	Name	Value			
Loof ISP	Summary				
	Name/Alias of the Connection Profile	SSL_GRP			
Home	VPN Access Interface	Internet			
orate	Device Digital Certificate	none			
Network	VPN Protocols Enabled	SSL only			
	AnyConnect Client Images	1 package			
Franker Ve	Authentication Server Group	LOCAL			
	Address Pool for the Client	10.10.10.1 - 10.10.10.200			
	DNS	Server: Domain Name:			
	Network Address Translation	The protected traffic is not subjected to network address translation			
[< Back Finish	Cancel Help			

AnyConnect客户端配置当前完成。然而,当您通过配置向导时配置AnyConnect,默认情况下它配置**认证方法作为AAA**。为了通过证书和用户名/密码验证客户端,必须配置隧道组(连接配置文件)使用证书和AAA作为认证方法。

- 连接对Configuration>远程访问VPN >网络(客户端)访问> AnyConnect连接配置文件。
- 您应该看到SSL_GRP列出的新的被添加的连接配置文件。

Device List 🗗 🖓 🗡	Configuration >	Remote Access VPN	> Network (Client)	Access > AnyConne	ect Connection Profiles				
	The security app tunnel with Data	iliance automatically dep gram Transport Layer So	loys the Cisco AnyCor ecurity (DTLS) tunnelir	nnect VPN Client to rem ng options.	ote users upon connection. Th	initial di	ent deployment requires end	I-user administrative rights. The Cisco AnyConn	ect VPN Client supports IPsec (IKEv2) tunnel as well as SSL
2	Enable Cisco SSL access must	AnyConnect VPN Client be enabled if you allow	access on the interfa AnyConnect client to	ices selected in the tabl be launched from a bro	e below wser (Web Launch) .				
	to be for a	SSL Access	SSL Access IPsec (IKEv2)		() Access				
	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services		Device Certificate]	
Remote Access VPN 🗗 🕀	Inside						Port Settings	1	
Introduction Network (Client) Access	Internet Outside					-			
AnyConnect Connection Profiles AnyConnect Customization (Localization AnyConnect Customization (Localization AnyConnect Clent Profile AnyConnect Clent Software Dynamic Access Policies Group Polices Dynamic Access Policies Secure Mobility Solution AnyConnect Software Advanced Advanced Advanced									
AnyConnect Essentials BanyConnect Custom Attributes Content Custom Attributes	Connection profile (turnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile tere.								
Clientless SSL VPN Access	Default0 A Creue	50	st chabled	IPS	ec chableu		Aldoes	Audientication Method	Office Delicy
Connection Profiles	DefaultWEBVPN	Group	(m)					AAA(LOCAL)	DftGrpPolicy
Portal	ssl-grp				v V		ssl-grp	AAA(LOCAL)	DfltGrpPolicy
	SSL_GRP		V		***		SSL_GRP	AAA(LOCAL)	GroupPolicy_SSL_GRP

•为了配置AAA和**证书验证**,选择连接配置文件SSL_GRP和点击**编辑**。

• 任 K ய J 本 F、,	tion Profile: SSL_GRP		X
· ·	-		
Basic	Name:	SSL_GRP	
Advanced	Aliases:	SSL_GRP	
	Authentication		
	Method:	AAA Certificate Both	
	AAA Server Group:	LOCAL Manage	••••
		Use LOCAL if Server Group fails	
	Client Address Assignment –		
	DHCP Servers:		
		None DHCP Link DHCP Subnet	
	Client Address Pools:	VPN_Pool Select.	
	Client IPv6 Address Pools:	Select.	
	Default Group Policy		
	Group Policy:	GroupPolicy_SSL_GRP Manage	••••
	Following field is an attribution of the second sec	ute or the group policy selected above.)	
	Enable IPsec(IKEv2)	client protocol	
	DNS Servers:		
	WINS Servers:		
	Domain Name:		
Find:	Ne	ext OPrevious	
	OK	Cancel Help	

配置AnyConnect的CLI

!! *****Configure the VPN Pool*****

ip local pool VPN_Pool 10.10.10.1-10.10.200 mask 255.255.255.0

!! *****Configure Address Objects for VPN Pool and Local Network*****

object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0
object network NETWORK_OBJ_192.168.10.0_24 subnet 192.168.10.0 255.255.255.0 exit !!
*****Configure WebVPN*****

webvpn enable Internet anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1 anyconnect enable tunnel-group-list enable exit **!!** *****Configure User****

username user1 password mb02jYs13AX1IAGa encrypted privilege 2

!! *****Configure Group-Policy*****

group-policy GroupPolicy_SSL_GRP internal group-policy GroupPolicy_SSL_GRP attributes vpntunnel-protocol ssl-client dns-server none wins-server none default-domain none exit !! *****Configure Tunnel-Group*****

tunnel-group SSL_GRP type remote-access tunnel-group SSL_GRP general-attributes authentication-server-group LOCAL default-group-policy GroupPolicy_SSL_GRP address-pool VPN_Pool tunnel-group SSL_GRP webvpn-attributes authentication aaa certificate group-alias SSL_GRP enable exit

!! *****Configure NAT-Exempt Policy*****

nat (Inside,Internet) 1 source static NETWORK_OBJ_192.168.10.0_24 NETWORK_OBJ_192.168.10.0_24
destination static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24 no-proxy-arp route-lookup

Verify

使用本部分可确认配置能否正常运行。

Note:<u>命令输出解释程序工具</u>(<u>仅限注册用户</u>)支持某些 show 命令。使用输出解释器工具来 查看 show 命令输出的分析。

保证CA服务器是启用的。

显示crypto加州服务器

ASA(config)# show crypto ca server Certificate Server LOCAL-CA-SERVER: Status: enabled

State: enabled

Server's configuration is locked (enter "shutdown" to unlock it)
Issuer name: CN=ASA.local
CA certificate fingerprint/thumbprint: (MD5)
 32e868b9 351a1b07 4b59cce5 704d6615
CA certificate fingerprint/thumbprint: (SHA1)
 6136511b 14aa1bbe 334c2659 ae7015a9 170a7c4d
Last certificate issued serial number: 0x1
CA certificate expiration timer: 19:25:42 UTC Jan 8 2019
CRL NextUpdate timer: 01:25:42 UTC Jan 10 2016
Current primary storage dir: flash:/LOCAL-CA-SERVER/

Auto-Rollover configured, overlap period 30 days Autorollover timer: 19:25:42 UTC Dec 9 2018

WARNING: Configuration has been modified and needs to be saved!! 保证用户允许登记在添加以后:

*****Before Enrollment*****

ASA# show crypto ca server user-db username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: 19:03:11 UTC Thu Jan 14 2016 notified: 1 times enrollment status: Allowed to Enroll >>> Shows the status "Allowed to Enroll"

*****After Enrollment*****

username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: 19:05:14 UTC Thu Jan 14 2016 notified: 1 times enrollment status: Enrolled, Certificate valid until 19:18:30 UTC Tue Jan 10 2017, Renewal: Allowed

您可以通过CLI或ASDM检查anyconnect连接的详细资料。

通过CLI

显示vpn-sessiondb详细资料anyconnect

ASA# show vpn-sessiondb detail anyconnect

```
Session Type: AnyConnect Detailed
```

Username : user1 Index : 1 Public IP Assigned IP : 10.10.10.1 : 10.142.189.181 : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel Protocol : AnyConnect Essentials License Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Tx : 13822 Bytes Rx : 13299 Pkts Tx : 10 Pkts Rx : 137 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : GroupPolicy_SSL_GRP Tunnel Group : SSL_GRP Login Time : 19:19:10 UTC Mon Jan 11 2016 : 0h:00m:47s Duration Inactivity : 0h:00m:00s

NAC Result : Unknown VLAN : none VLAN Mapping : N/A AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 1.1 Public IP : 10.142.189.181 Encryption : none Hashing : none TCP Src Port : 52442 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096 Bytes Tx : 6911 Bytes Rx : 768 Pkts Tx : 5 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 1.2 Assigned IP : 10.10.10.1 Public IP : 10.142.189.181 Hashing : SHA1 Encryption : RC4 TCP Src Port : 52443 Encapsulation: TLSv1.0 Auth Mode : Certificate and userPassword Idle TO Left : 29 Minutes TCP Dst Port : 443 Idle Time Out: 30 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096 Bytes Tx : 6911 Bytes Rx : 152 Pkts Rx : 2 Pkts Tx : 5 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 1.3 Assigned IP : 10.10.10.1 Public IP : 10.142.189.181 Encryption : AES128 Hashing : SHA1 UDP Src Port : 59167 Encapsulation: DTLSv1.0 Auth Mode : Certificate and userPassword Idle TO Left : 30 Minutes UDP Dst Port : 443 Idle Time Out: 30 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096 Bytes Tx : 0 Bytes Rx : 12907 Pkts Tx : 0 Pkts Rx : 142 Pkts Tx Drop : 0 Pkts Rx Drop : 0 NAC: Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds SQ Int (T) : 0 Seconds EoU Age(T) : 51 Seconds Hold Left (T): 0 Seconds Posture Token: Redirect URL :

通过ASDM

- 连接对Monitoring> VPN > VPN统计数据>会话。
- •由作为**所有远程访问**选择过滤器。
- 您可以进行所选的AnyConnect客户端的动作之一。 详细资料提供关于会话的更多信息

退出手工退出从数据转发器的用户

连接从数据转发器连接AnyConnect客户端

Filter By: All Remote A	ccess 👻	All Sessions	•	Filter	
Username	Group Policy Connection Profile	Public IP Address Assigned IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
user 1	ssl-pol ssl-grp	10.142.189.80 192.168.1.1	AnyConnect-Parent AnyConnect-Parent	t SSL-Tunnel DTLS 14:39:08 UTC Mo t: (1)none SSL-Tu 0h:00m:33s	. 10998 885

Troubleshoot

本部分提供了可用于对配置进行故障排除的信息。

Note:使用 debug 命令之前,请参阅<u>有关 Debug 命令的重要信息</u>。

警告:在ASA,您能设置多种调试级别;默认情况下,使用第1级。如果更改调试级别,调试的 冗余也许增加。执行此小心地,特别是在生产环境里。

- · debug crypto ca
- debug crypto ca服务器
- debug crypto ca消息
- debug crypto ca处理
- 调试WebVPN anyconnect

当CA服务器使用no shut命令,是启用的此调试输出显示。

ASA# debug crypto ca 255 ASA# debug crypto ca server 255 ASA# debug crypto ca message 255 ASA# debug crypto ca transaction 255 CRYPTO_CS: input signal enqueued: no shut >>>>> Command issued to Enable the CA server Crypto CS thread wakes up! CRYPTO_CS: enter FSM: input state disabled, input signal no shut CRYPTO_CS: starting enabling checks CRYPTO_CS: found existing serial file. CRYPTO_CS: started CA cert timer, expiration time is 17:53:33 UTC Jan 13 2019 CRYPTO_CS: Using existing trustpoint 'LOCAL-CA-SERVER' and CA certificate CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser CRYPTO_CS: DB version 1 CRYPTO_CS: last issued serial number is 0x4 CRYPTO_CS: closed ser file CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.crl CRYPTO_CS: CRL file LOCAL-CA-SERVER.crl exists. CRYPTO_CS: Read 220 bytes from crl file. CRYPTO_CS: closed crl file CRYPTO_PKI: Storage context locked by thread Crypto CA Server CRYPTO_PKI: inserting CRL CRYPTO_PKI: set CRL update timer with delay: 20250 CRYPTO_PKI: the current device time: 18:05:17 UTC Jan 16 2016

CRYPTO_PKI: the last CRL update time: 17:42:47 UTC Jan 16 2016 CRYPTO_PKI: the next CRL update time: 23:42:47 UTC Jan 16 2016 CRYPTO_PKI: CRL cache delay being set to: 20250000 CRYPTO_PKI: Storage context released by thread Crypto CA Server

CRYPTO_CS: Inserted Local CA CRL into cache!

CRYPTO_CS: shadow not configured; look for shadow cert CRYPTO_CS: failed to find shadow cert in the db CRYPTO_CS: set shadow generation timer CRYPTO_CS: shadow generation timer has been set CRYPTO_CS: Enabled CS. CRYPTO_CS: exit FSM: new state enabled CRYPTO_CS: cs config has been locked.

Crypto CS thread sleeps!

此调试输出显示客户端的登记

```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255
```

CRYPTO_CS: writing serial number 0x2. CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser CRYPTO_CS: Writing 32 bytes to ser file CRYPTO_CS: Generated and saving a PKCS12 file for user user1 at flash:/LOCAL-CA-SERVER/user1.p12

客户端的登记可能失效在这些conditons下:

方案1。

•用户在CA服务器数据库被创建,不用权限登记。

🔁 Add User		×
Username:	user 1	
Email ID:	user1@cisco.com	
Subject (DN String):	CN=user1,OU=TAC	Select
Allow enrollment		
	Add User Cancel Help	

等效的 CLI 命令:

ASA(config) # show crypto ca server user-db

username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC • 在用户不允许登记的案件,尝试生成/电子邮件用户的OTP生成此错误信息。



场景2:

•验证端口并且建立接口在哪些登记门户是可用的使用webvpn命令的show run。默认端口是 443,但是可以被修改。

•保证客户端有网络可达性对WebVPN在用于的端口被启用顺利地访问登记门户接口的IP地址。 客户端可能不能在这些情况下访问ASA登记门户:

- 1. 如果任何中间设备阻拦从客户端的流入的连接与ASA的WebVPN IP在端口的指定的。
- 2. 接口的状态下降在哪WebVPN是启用的。
- 此输出表示,登记门户是可用的在接口互联网的IP地址自定义端口的4433。

ASA(config) # show run webvpn webvpn port 4433 enable Internet no anyconnect-essentials anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1 anyconnect enable tunnel-group-list enable

场景3:

- CA服务器数据库存贮的默认位置是ASA的闪存。
- •保证闪存有空闲空间生成和保存用户的pkcs12文件在登记期间。
- 在闪存没有足够的空闲空间的案件, ASA不能完成客户端的登记进程并且生成这些调试日志:

ASA(config)# debug crypto ca 255 ASA(config)# debug crypto ca server 255 ASA(config)# debug crypto ca message 255 ASA(config)# debug crypto ca transaction 255 ASA(config)# debug crypto ca trustpool 255 CRYPTO_CS: writing serial number 0x2. CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser CRYPTO_CS: Writing 32 bytes to ser file CRYPTO_CS: Generated and saving a PKCS12 file for user user1 at flash:/LOCAL-CA-SERVER/user1.p12

CRYPTO_CS: Failed to write to opened PKCS12 file for user user1, fd: 0, status: -1.

CRYPTO_CS: Failed to generate pkcs12 file for user user1 status: -1.

CRYPTO_CS: Failed to process enrollment in-line for user user1. status: -1

Related Information

- Cisco ASA 5500 系列自适应安全设备
- AnyConnect VPN 客户端故障排除指南 常见问题
- 管理,监控和排除AnyConnect会话故障
- Technical Support & Documentation Cisco Systems