ASA 8.x:适用于Windows的AnyConnect SSL VPN CAC智能卡配置

目录
<u>简介</u>
先决条件
<u>要求</u>
使用的组件
<u>Cisco ASA 配置</u>
<u>部署注意事项</u>
<u>认证,授权,计费(AAA)配置</u>
<u>配置 LDAP 服务器</u>
<u>管理证书</u>
<u>生成密钥</u>
<u>安装根 CA 证书</u>
<u>注册 ASA 并安装身份证书</u>
AnyConnect VPN 配置
<u>创建 IP 地址池</u>
创建隧道组和组策略
<u>隧道组界面和镜像设置</u>
<u>证书匹配规则(如果将使用 OCSP)</u>
配置 OCSP
配置 OCSP Responder 证书
配置 CA 以使用 OCSP
配置 OCSP 规则
<u> Cisco AnyConnect Client 配置</u>
<u>下载 Cisco Anyconnect VPN 客户端 - Windows</u>
<u>启动 Cisco AnyConnect VPN 客户端 - Windows</u>
新建连接
<u>启动远程访问</u>
<u>附录 A - LDAP 映射和 DAP</u>
<u>方案1:使用远程访问权限拨入实施Active Directory -允许/拒绝访问</u>
<u>活动目录设置</u>
ASA 配置
<u>方案2:使用组成员身份允许/拒绝访问的Active Directory实施</u>
<u>活动目录设置</u>
ASA 配置
<u>场景3:多个memberOf属性的动态访问策略</u>
ASA 配置
<u>附录 B - ASA CLI 配置</u>

 M录C-故障排除

 AAA和LDAP故障排除

 示例1:具有正确属性映射的允许连接

 示例1:具有正确属性映射的允许连接

 示例2:思科属性映射配置错误的允许连接

 DAP故障排除

 示例1:允许与DAP的连接

 示例2:与DAP的连接被拒绝

 故障排除认证中心/OCSP

 附录D-在MS中验证LDAP对象

 LDAP查看器

 适动目录服务接口编辑器

 附录E

简介

本文档提供在 Windows 环境下,在 Cisco 自适应安全设备 (ASA) 上针对 AnyConnect VPN 远程访问进行配置的示例,其中使用通用访问卡 (CAC) 进行身份验证。

本文档涵盖具有自适应安全设备管理器(ASDM)、Cisco AnyConnect VPN客户端和Microsoft Active Directory (AD)/轻量级目录访问协议(LDAP)的Cisco ASA的配置。

本指南中的配置使用 Microsoft AD/LDAP 服务器。本文档还介绍了OCSP、LDAP属性映射和动态 访问策略(DAP)等高级功能。

先决条件

要求

基本了解Cisco ASA、Cisco AnyConnect客户端、Microsoft AD/LDAP和公钥基础设施(PKI)有助于 理解完整设置。熟悉 AD 组成员、用户属性以及 LDAP 对象有助于了解证书属性和 AD/LDAP 对象 的授权过程之间的相互关系。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 以后Cisco 5500系列可适应的安全工具(ASA)该运行软件版本8.0(x)和
- ASA的8.x Cisco Adaptive Security Device Manager (ASDM) 6.x版
- 适用于 Windows 的 Cisco AnyConnect VPN 客户端

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

Cisco ASA 配置

本部分包括通过 ASDM 配置 Cisco ASA 的内容。其中介绍了用于部署使用 SSL AnyConnect 连接 的 VPN 远程访问隧道所需的步骤。CAC证书用于身份验证,并且证书中的用户主体名称(UPN)属性 填充在active directory中以进行授权。

部署注意事项

 本指南不讨论基本配置内容,例如接口、DNS、NTP、路由、设备访问、ASDM 访问等。假 定网络操作员已熟悉这些配置。

有关详细信息,请参阅多功能安全设备。

- 红色突出显示的部分为基本 VPN 访问所必需的配置。例如,可以使用CAC卡设置VPN隧道 ,而无需执行OCSP检查、LDAP映射和动态访问策略(DAP)检查。DoD 需要执行 OCSP 检查
 - ,但是隧道无需配置 OCSP 也可工作。
- 蓝色突出显示的部分是可选的高级功能,此功能可以增强设计的安全性。
- ASDM 和 AnyConnect/SSL VPN 不能使用相同接口上的相同端口。建议更改任意一个接口上的端口以便可以进行访问。例如,将端口 445 用于 ASDM,而将 443 用于 AC/SSL VPN。在 8.x. 版本中,ASDM URL 访问已发生变化。请使用https://<ip_address>:<port>/admin.html。
- 所需的 ASA 映像的版本至少为 8.0.2.19,并且需要 ASDM 6.0.2。
- AnyConnect/CAC 受 Vista 支持。
- 有关更多策略实施的 LDAP 和动态访问策略映射示例,请参阅<u>附录 A</u>。
- 有关如何在MS中检查LDAP对象,请参阅<u>附录D</u>。
- 有关用于防火墙配置的应用程序端口列表,请参阅相关信息。

认证,授权,计费(AAA)配置

您使用通用访问卡(CAC)中的证书通过证书颁发机构(CA)服务器或他们自己组织的CA服务器进行身份验证。证书必须对远程网络访问有效。除身份验证外,还必须授权您使用Microsoft Active Directory或轻量级目录访问协议(LDAP)对象。国防部(DoD)需要使用用户主体名称(UPN)属性进行授权,这是证书的使用者备用名称(SAN)部分的一部分。UPN 或 EDI/PI 必须遵循 1234567890@mil 格式。这些配置显示了如何在 ASA 中通过 LDAP 服务器(用于授权)来配置AAA 服务器。有关通过 LDAP 对象映射进行的其他配置,请参阅<u>附录 A。</u>

配置 LDAP 服务器

请完成以下步骤:

1. 选择 Remote Access VPN > AAA Setup > AAA Server Group。

- 2. 在 AAA 服务器组表中,单击 Add 3。
- 3. 输入服务器组名称,并选择 LDAP 协议单选按钮。请参阅图 1。
- 4. 在所选组表的服务器中,单击 Add。确保所创建的服务器在前一张表中处于突出显示状态。
- 5. 在编辑 AAA 服务器窗口中,执行以下步骤。请参阅图 2。

注意:如果已针对此类连接配置了LDAP/AD,请选择Enable LDAP over SSL选项。

- a. 选择 LDAP 所处的接口。本指南显示接口内部。
- b. 输入服务器的 IP 地址。
- c. 输入 Server Port。默认的 LDAP 端口是 389。
- d. 选择 Server Type。
- e. 输入 Base DN。请向 AD/LDAP 管理员咨询这些值。

图-1

🖆 Add AAA Server Group			
Configure an AAA ser for RADIUS and TACA	ver group. The Accounting Mode attribute is only applicable \CS+ protocols.		
Server Group:	AD-LDAP		
Protocol:	LDAP		
Accounting Mode:	🔄 Simultaneous 🔅 Single		
Reactivation Mode:	Oppletion O Timed		
Dead Time: 10	Minutes		
Max Failed Attempts:	3		

- f. 在 Scope 选项下,选择适当的答案。这取决于 Base DN。请向 AD/LDAP 管理员寻求帮助。
- g. 在 Naming Attribute 中,输入 userPrincipalName。这是 AD/LDAP 服务器中用于用户授权的属性。

h. 在 Login DN 中,输入管理员 DN。

注意:您拥有查看/搜索包括用户对象和组成员资格的LDAP结构的管理权限或权限。

- i. 在 Login Password 中,输入管理员的口令。
- j. 保留 LDAP 属性的默认设置 none。

图-2

🚰 Add AAA Server			×
Server Group:		AD-LDAP	
Interface Name:		outside]
Server Name or IP Address:		172.18.120.160]
Timeout:		10	seconds
LDAP Parameters			
Enable LDAP over SSL			
Server Port:	389		
Server Type:	Detect Automatically/Use Generic Type 💟		
Base DN:	CN=Users,DC=ggsgseclab,DC=org		
Scope:	One level beneath the Base DN		
Naming Attribute(s):	userPrincipalName		
Login DN:	lministrator, CN=Users, DC=ggsgseclab, DC=org		
Login Password:			
LDAP Attribute Map:	None		
SASL MD5 authentication			
5ASL Kerberos authentication			

注意:稍后在配置中使用此选项来添加其他AD/LDAP对象以进行授权。

k. 选择 OK。

6. 选择 OK。

管理证书

要在 ASA 上安装证书,需要执行两个步骤。首先,安装所需的 CA 证书(根证书机构和辅助证书机 构)。其次,请向特定的 CA 登记 ASA,并获取身份证书。DoD PKI 使用以下证书:Root CA2、 Class 3 Root、ASA 登记所使用的 CA## Intermediate、ASA ID 证书和 OCSP 证书。但是,如果选 择不使用 OCSP,则不 需要安装 OCSP 证书。

注意:请与您的安全POC联系以获得根证书以及如何注册设备的身份证书的说明。SSL 证书 应该能够满足 ASA 进行远程访问。无需 双重 SAN 证书。

注意:本地计算机还必须安装DoD CA链。可以使用 Internet Explorer 在 Microsoft Certificate Store 中查看证书。DoD 设计了一个批处理文件,它可以自动将所有 CA 添加到计算机中。有 关详细信息,请咨询 PKI POC。

注意:DoD CA2和3类根以及颁发ASA证书的ASA ID和CA中间证书应为用户身份验证所需的 唯一CA。当前所有中间 CA 都位于 CA2 和 Class 3 Root 链之下,只要添加了 CA2 和 Class 3 Root,这些中间 CA 都将成为可信 CA。

生成密钥

请完成以下步骤:

- 1. 选择 Remote Access VPN > Certificate Management > Identity Certificate > Add。
- 2. 选择 Add a new id certificate, 然后选择密钥对选项旁边的 New。
- 在 Add Key Pair 窗口中,输入密钥名称 DOD1024。单击单选按钮以添加新密钥。请参阅图
 3。

图 3

🕵 Add K	ey Pair	
Name:	🚫 Use default key pair name	
	💿 Enter new key pair name:	DoD-1024
Size:	1024	
1		

- 4. 选择密钥的大小。
- 5. 保留 Usage 的默认设置 General Purpose。
- 6. 单击 Generate Now。

注意:DoD根CA 2使用2048位密钥。应生成第二个使用2048位密钥对的密钥,以便能 够使用此CA。完成上述步骤以添加第二个密钥。

安装根 CA 证书

请完成以下步骤:

- 1. 选择 Remote Access VPN > Certificate Management > CA Certificate > Add。
- 2. 选择 Install from File,并浏览到相应证书。
- 3. 选择 Install Certificate。

图4:安装根证书

🖆 Install Certificate		
 Install from a file: 	C:\CAC\DOD-CERTS\ca13-jitc.ce	Browse
O Paste certificate in	PEM format:	
O Use SCEP:		
SCEP URL: http://		
Retry Period:	1	minutes
Retry Count:	0	(Use 0 to indicate unlimited retries)
		More Options
Install Ce	rtificate Cancel	Help

4. 应出现以下窗口。请参阅图 5。

图 5

🗲 CA Certi	ficate Installation 🔀
į	CA certificate installed successfully.
	OK

注意:对要安装的每个证书重复步骤1到3。DoD PKI要求为以下各项提供证书:根CA 2、类3 Root、CA## Intermediate、ASA ID和OCSP Server。如果不使用 OCSP,则不 需要 OCSP 证书。

图6:安装根证书

tempte Acces VPN 🚊 4 🕉	Configuration > Rean	te Access VPN.). Contificate Man	agement > EA Certificates	
Ketwork (Client) Access				
🚽 🖬 AAA Geb p	Issued To	Jesued Sy	Excity Date Usage	bhé
🔒 Seture Ceskuut Manager 🔝 Freitrichte Monogement	DeD Rock CA 2 DeD CLASS 0 Root CA	[[umbld Root CA2, LumPit, Lum [[m=0::001455 - Root (A) oue is a	15:00:10 UTC Signature 10:01-311/110 General Purpose	l dit
	000 JTC CA-13	[ui=DLC DITC Roll CA 2, lu≑PK1	C2:55:53 UTC Signature	how 24th
En Cope Signer E Kin Local Certificate Authority				Req esta
📲 Load Talancing				Delete
A [®] CHCP Server ■ CNS ■ CNS				
Device Set_p				
Firewel				

注册 ASA 并安装身份证书

- 1. 选择 Remote Access VPN > Certificate Management > Identity Certificate > Add。
- 2. 选择 Add a new id certificate。
- 3. 选择 DoD-1024 密钥对。请参阅图 7。

图7:身份证书参数

🚰 Add Identity Certifical	e	
 Import the identity certif 	icate from a file:	
Decryption Passphrase:		
File to Import From:		Browse
 Add a new identity certif 	icate:	
Key Pair:	DoD-1024	Show New
Certificate Subject DN:		Select
Generate self-signed	certificate	
Act as local certif	icate authority and issue dynamic ce	artificates to TLS-Proxy
		Advanced
Add Certifi	cate Cancel	Help

- 4. 转到 Certificate subject DN 框,并单击 Select。
- 5. 在 Certificate Subject DN 窗口中,输入设备的信息。有关示例,请参阅图 8。
 - 图8:编辑DN

DN Attribute to be Added Attribute Value Attribute: Select Attribute Add>> Department (OU) PKI Department (OU) DoD
DN Attribute to be Added Common Name (CN) asa80 Attribute: Select Attribute Add>> Department (OU) PKI
DN Attribute to be Added Department (OU) PKI Attribute: Select Attribute Add>> Department (OU) DoD
Attribute: Select Attribute 🔽 Add>> Department (OU) DoD
Company Name (O) U.S. Governme
Value: Delete Country (C) US

6. 选择 OK。

注意:请确保在添加主题DN时使用系统中配置的设备主机名。PKI POC 会告知您哪些 字段必须填写。

- 7. 选择 Add certificate。
- 8. 单击 Browse,以选择要保存请求的目录位置。请参阅图 9。

图9:证书请求

🖾 Identity Certificate Request	
To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.	
You will then need to install the certificate that is returned from the CA by	

9. 使用 Wordpad 打开文件,将请求复制到相应的文档中,并发送给 PKI POC。请参阅图 10。

图10:注册请求

ASA-8.0 - WordPad	
File Edit View Insert Format Help	- an an an an
□ ☞ 🖬 🔿 🖪 🔺 🗴 ๒ 🛍 ∽ 🔍	
<pre>MIIB1TCB/wIBADAmMQ4wDAYDVQQDEwVhc2E4MDEUMBIGCSqGSIb3DQEJAhYFYXNh ODAwg28wDQYJKoZIhvcNAQEBBQADgYOAMIGJAoGBAJqhuFdN12G7J3GCMcQ4KT27 skELghwrraRMeB9iFJnLy10JYaUSAOvcededpeIUF7jUHYoIxS3v0Eby1VdvN75A +Z0DfU+wc1U+aA25yc6TnixGxppgxNYSU+4j6pgwui86Rk1+7BbVnJnJ+f3EKc1t pMzBix7GetFRA8JsVvzvAgMBAAGgMDAuBgkqhkiG9w0BCQ4xITAfMAsGA1UdDwQE AwIFoDAQBgNVHREECTAHggVhc2E4MDANBgkqhkiG9w0BAQQFAAOBgQBmf8xSnVTw QQF7TuEaUhmVaKfOBhupf+Y0Fm9Xt8T3GSSj1H/t+XB2cyLzNSthu2FVr5m97cT9 jw31+jHv57zB1uDH3AYkM+Hru4yzgqBrgQBMCDIpmyCRp0EZpn2QaX/cD0xkqpv8 KgfJHq+2x3eVgvSxyKfhE71yFN3ResrSTg==</pre>	

- 10. 从 CA 管理员处收到证书之后,请选择 Remote Access VPN > Certificate Management > ID Certificate > Install。请参阅图 11。
 - 图11:导入身份证书

🚰 Add IP Pool	
	P
Name:	CAC-USERS
Starting IP Address:	192,168,1,1
Ending IP Address:	192,168.1,254
Subnet Mask:	255.255.255.0
ОК	Cancel Help

11. 在 Install certificate 窗口中,浏览到该 ID 证书,并选择 Install Certificate。有关示例,请参阅 图 12。

图12:安装身份证书

🖆 Install Identity ce	rtificate	<u> </u>
Identity Certificate	CUCACIDOD-CERTSJaka80.tvt	Browse
 Paste the certificat 	e data in base-64 format:	
		Heip

注意:建议导出ID证书信任点,以保存颁发的证书和密钥对。这样,当出现 RMA 或硬件故障时,ASA 管理员可将证书和密钥对导入到新的 ASA 中。有关详细信息,请参阅 <u>导出和导入信任点。</u>

注意:单击SAVE,以将配置保存在闪存中。

AnyConnect VPN 配置

在 ASDM 中,有两种方式可用于配置 VPN 参数。第一种方式是使用 SSL VPN 向导。该工具易于 使用,适用于不熟悉 VPN 配置的用户。第二种方式是手动配置每个选项。本配置指南采用手动方 式。

注意:有两种方法可将AC客户端提供给用户:

1. 从 Cisco 网站上下载客户端,并将其安装到计算机上。

2. 通过 Web 浏览器访问 ASA, 然后下载客户端。

注意:例如,<u>https://asa.test.com</u>。本指南使用第二种方法。将 AC 客户端永久安装到客户端 计算机后,您只需从应用程序中启动 AC 客户端即可。

创建 IP 地址池

如果您使用其他方法(如 DHCP),则此操作是可选的。

- 1. 选择 Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools。
- 2. 单击 Add。
- 3. 在 Add IP Pool 窗口中,输入 IP 池的名称、起始 IP 地址和结束 IP 地址,并选择一个子网掩 码。请参阅图 13。

图13:添加IP池

🖆 Add IP Pool	X
Name:	CAC-USERS
Starting IP Address:	192.168.1.1
Ending IP Address:	192,168,1,254
Subnet Mask:	255.255.255.0
ОК	Cancel Help

- 4. 选择 OK。
- 5. 选择 Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy。
- 6. 选择适当的 IP 地址分配方法。本指南使用内部地址池。请参阅图 14。

图14:IP地址分配方法



7. 单击 Apply。

创建隧道组和组策略

组策略

注意:如果不想创建新策略,则可以使用默认的内置组策略。

- 1. 选择 Remote Access VPN -> Network (Client) Access -> Group Policies。
- 2. 单击 Add, 然后选择 Internal Group Policy。
- 3. 在添加内部组制度窗口,请输入名称对于组制度在命名文本框。请参阅图 15。
 - 图15:添加内部组策略

General	Name: A	C-USERS					
Advanced	Banner:	Inherit					
	Address Pools: [Inherit	CAC-USE	ণ্ড			Select
	More Options						۲
	Tunneling Proto	cols: [🗌 Inherit	Clientless SSL VPN	SSL VPN Client	IPsec	L2TP/IPsec
	Filter:	[🗹 Inherit				Manage
	NAC Policy:	[🖌 Inherit			×.	Manage
	Access Hours:	[🖌 Inherit			2	Manage
	Simultaneous Lo	gins: [🗹 Inherit				
	Restrict access	to VLAN: [Inherit				
	Maximum Conne	ect Time: [🖌 Inherit	Unimited	mnutes		
	Ide Timeout:	[🔽 Inherit	Unimited	mnubes		

- a. 在 General 选项卡上,选择 SSL VPN Client in the Tunneling Protocols 选项,除非您使 用其他协议(如 Clientless SSL)。
- b. 在 Servers 部分中,取消选中 Inherit 复选框,并输入 DNS 和 WINS 服务器的 IP 地址 。如果适用,输入 DHCP 范围。
- c. 在 Servers 部分中,取消选中 Default Domain 中的 inherit 复选框,并输入适当的域名。
- d. 在 General 选项卡上,取消选中 Address Pool 部分中的 Inherit 复选框,并添加在上一步创建的地址池。如果您使用另一种 IP 地址分配方法,请保留 Inherit 的默认状态,并 作相应的更改。
- e. 所有其他配置选项卡均保留默认设置。

注意:有两种方法可将交流客户端提供给最终用户。一种方法是从 Cisco.com 上 下载 AC 客户端。第二种方法是在用户尝试进行连接时,由 ASA 为用户下载客户 端。本示例使用后一种方法。

4. 然后,选择 Advanced > SSL VPN Client > Login Settings。请参阅图 16。

图16:添加内部组策略

📬 Edit Internal Group Pol	icy: AC-USERS	×
General Servers Advanced Split Tunneling E Browser Proxy SSL VPN Clent Cogn Settino Dead Peer Detecto Customization F-IPsec Clent	After successfully logging in, user can have the choice to download the client software, or go to clientless SSL VPN portal page. The following settings decides what will happen. Inherit Post Logn Setting Point prompt user to choose User has	
	OK Cancel Help	

a. 取消选中 Inherit 复选框。

b. 选择与您的环境相应的 Post Login Setting。

c. 选择与您的环境相应的 Default Post Login Selection。

d. 选择 OK。

隧道组界面和镜像设置

注意:如果不想创建新组,则可以使用默认的内置组。

- 1. 选择 Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile。
- 2. 选择 Enable Cisco AnyConnect Client.....。
- 3. 即会出现一个对话框,询问您 Would you like to designate an SVC image?
- 4. 选择 Yes。
- 5. 如果已存在映像,请通过 Browse Flash 选择该映像。如果不存在映像,请选择 Upload,并浏 览到本地计算机上的文件。请参阅图 17。文件可以从Cisco.com下载;有Windows、MAC和 Linux文件。

🚰 Add SSL VPN Client Image	<u> </u>
Flash SVC Image:	Browse Flash
	Upload

6. 然后启用 Allow Access、Require Client Cert,并根据需要启用 Enable DTLS。请参阅图 18。

图18:启用访问

📫 Cisco ASDM 6.0 for ASA - 172	2.18.120.225				
Ele View Icols Wigards Window	w Help Ionitoring 📑 Save	🐼 Refresh	Look For: Back Of Forward ? Help	find +	ahaha cisco
Remote Access V A X	Configuration > Re The security applia users upon connect VPN Clent supports (More clent-relate Access Interfaces C Enable Cisco A Interface cutside	Inde Access VPN Ince automatically dep tion. The initial client of the HTTPS/TCP (SSL diparamaters, such a hyConnect VPN Client Allow Access	> Network (Client) Access > S loys the Cisco AnyConnect VPN Client deployment requires end-user admin) and Dabagram Transport Layer Set is client images and client profiles, ca or legacy SSL VPN Client access on Require Client Certificate	SL VPN Connection At or legacy SSL VPN Cli- strative rights. The Cls curity (DTLS) tunneling is in be found at <u>client Sec</u> the interfaces selected Enable DTLS	Profiles ent to remote co AnyConnect options. ttinos.) in the table below
	Access Port: 443 Click here to Asso Connection Profiles	DTLS Po n Certificate to Interf	rt: 443 308; Apply Reset		

- 7. 单击 Apply。
- 8. 然后,创建一个连接配置文件/隧道组。选择 Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile。

9. 在 Connection Profiles 部分中,单击 Add。

图19:添加连接配置文件

🖆 Add SSL VPN Connecti	ion Profile		X
Basic	Name:	AC-USERS	
H-Advanced	Aliases:		
	Authentication		
	Method:	◯ AAA ④ Certificate ◯ Both	
	AAA Server Group:	LOCAL	Manage
		Use LOCAL if Server Group Fails	
	Client Address Assignment		
	DHCP Servers:		
	Client Address Pools:		Select
	Default Group Policy		
	Group Policy:	AC-USER5	Manage
	SSL VPN Client Protocol:	C Enabled	
000000000000000000000000000000000000000	J		
	OK	Cancel Help	

- a. 为该组命名。
- b. 在身份验证方法中选择 Certificate。
- c. 选择之前创建的组策略。
- d. 确保启用 SSL VPN Client。
- e. 其他选项保留默认状态。
- 10. 然后,选择 Advanced > Authorization。请参阅图 20。
 - 图20:授权

💕 Edit SSL VPN Connecti	on Profile: AC-USER	S		
Basic Advanced General Client Addressing Authentication Accounting SSL VPN	Default Authorization Se Server Group: AD-LD V Us Interface-specific Author Add E Edt I Interface	erver Group DAP ers must exist in the ar rization Server Groups Delete	Anage Athorization database to connect Server Group	
	User Name Mapping Use the entire DN O Specify individual	as the username DN fields as the userna	me	
	Secondary DN Fiel	Id: None Cancel	Help	

a. 选择之前创建的 AD-LDAP 组。

b. 选中Users must exist...to connect。

c. 在映射字段中,分别为主字段和辅字段选择 UPN 和 None。

11. 选择菜单项 SSL VPN。

12. 在 Connection Aliases 部分中,执行以下步骤:

图21:连接别名

🖆 Edit SSL VPN Connecti	on Profile: AC-USERS		X		
Basic	Portal Page Customization:	DfltCustomization	Manage		
General	CSD Alternate Group Policy:	DfltGrpPolicy	Manage		
Client Addressing Authentication	Enable the display of Radius Reject-Message on the login screen when authentication is rejected				
Authorization Accounting	Connection Aliases				
SSL VPN	🗣 Add 🖪 Delete				
	Alias	is Enabled			
	AC-USERS				
	Group URLs				
	Add 🖬 Delete				
	URL	Enabled			
]				
	OK (Cancel Help			

a. 选择 Add。

b. 输入您要使用的组别名。

c. 确保选中 Enabled。请参阅图 21。

13. Click OK.

注意:单击Save,以将配置保存在闪存中。

证书匹配规则(如果将使用 OCSP)

- 1. 选择 Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps。 请参阅图 22。
 - a. 在 Certificate to Connection Profile Maps 部分中,选择 Add。
 - b. 在 Map 部分中,您可保留已有映射的 DefaultCertificateMap 配置,或新建一个映射 (如果已将证书映射用于 IPsec)。
 - c. 规则优先级保持默认。
 - d. 在映射组下,保留为— Not Mapped —。请参阅图 22。

Configure a certificate M Configure a certificate rule priority uniquely id to the rule with lower y will be ignored.	atching Rule matching rule and assoc lentifies the certificate m values having greater pri	iate it with a connection profile. The atching rule and assigns a priority ority. Rules that are not mapped
Map:	Existing	DefaultCertificateMap
	🚫 New	
Priority:	20	
Mapped to Connection	Profile: Not Mapped	
		2 (

- e. Click OK.
- 2. 在底部表上单击 Add。
- 3. 在 Add certificate Matching Rule Criterion 窗口中,执行以下步骤:

图23:证书匹配规则条件

Choose a	digital certificate		? 🔀
	ation The Web site you want to identification. Please cho	o view requests ose a certificate.	
	Name POOLE.JUSTIN.ALLE MCGINTY.JIMMY.11 POOLE.JUSTIN.ALLE MCGINTY.JIMMY.11	Issuer DOD CLASS 3 EMAIL CA-10 DOD JITC CA-15 DOD CLASS 3 CA-10 DOD JITC EMAIL CA-15	
	Mo	re Info View Certifical	te

- a. 保留 Field 列的默认值 Subject。
- b. 保留 Component 列的默认值 Whole Field。
- c. 将 Operator 列改为 Does Not Equal。
- d. 在 Value 列中,输入两个双引号""。
- e. 单击 OK,然后单击 Apply。有关示例,请参阅图 23。

配置 OCSP

OCSP 的配置可能会有所不同,这取决于 OCSP Responder 供应商。有关详细信息,请参阅供应 商手册。

配置 OCSP Responder 证书

1. 从 OCSP Responder 获取自生成的证书。

2. 执行前述步骤,并为 OSCP 服务器安装证书。

注意:确保为OCSP证书信任点选择了Do not check certificates for revocation。

配置 CA 以使用 OCSP

- 1. 选择 Remote Access VPN> Certificate Management > CA Certificates。
- 2. 突出显示 OCSP,以选择要配置使用 OCSP 的 CA。
- 3. 单击 Edit。
- 4. 确保选中 Check certificate for revocation。
- 5. 在 Revocation Methods 部分中,添加 OCSP。请参阅图 24。

OCSP撤销检查

evocation Check CRL Re	trieval Policy CRL Retrieval Method OCSP Rules A	dvanced
O Do not check certificat	es for revocation	
 Check certificates for it 	evocation	
Revocation Methods		
Specify the methods method will be used	used for revocation checking and their order. If both r only if the first one returns error.	nethods are selected, the second
CRL	Add>> OCSP	Move Up
	< <remove< td=""><td>Move Down</td></remove<>	Move Down
Consider contific	he uside a concentre information correct be extrinued	
	ate valid il revocadori il contracion cannoc de retrieved	

6. 如果要遵循严格的 OCSP 检查,请确保取消选中 Consider Certificate valid…cannot be retrieved。

注意:配置/编辑使用OCSP撤销的所有CA服务器。

注意:在完成这些步骤之前,请确认已创建证书组匹配策略并且已配置OCSP响应器。

注意:在某些OCSP实施中,ASA可能需要DNS A和PTR记录。此项检查目的在于确认 ASA 来自 .mil 站点。

1. 选择 Remote Access VPN> Certificate Management > CA Certificates 2。

- 2. 突出显示 OCSP,以选择要配置使用 OCSP 的 CA。
- 3. 选择 Edit。
- 4. 单击 OCSP Rule 选项卡。
- 5. 单击 Add。
- 6. 在 Add OCSP Rule 窗口中,执行以下步骤。请参阅图 25。

图25:添加OCSP规则

🕵 Add OCSP I	Rule	
Certificate Map:	DefaultCertificateMap	~
Certificate:	[ch=OCSP, ou=AMHS, o=Army, c=us]:[ch=OCSP, ou=AMHS	~

- a. 在 Certificate Map 选项中,选择 DefaultCertificateMap 或之前创建的映射。
- b. 在 Certificate 选项中,选择 OCSP responder。
- c. 在索引选择,请输入10。
- d. 在 URL 选项中,输入 IP 地址或 OCSP Responder 的主机名。如果使用主机名,请确 保已在 ASA 中配置了 DNS 服务器。
- e. Click OK.
- f. 单击 Apply。

Cisco AnyConnect Client 配置

本部分包括 Cisco AnyConnect VPN 客户端的配置。

假设 -主机PC中已安装Cisco AnyConnect VPN客户端和中间件应用程序。已测试 ActivCard Gold 和 ActivClient。

注意:本指南仅对初始AC客户端安装使用group-url方法。安装好 AC 客户端后,您可像启动 IPSec 客户端一样启动 AC 应用程序。

注意:需要在本地计算机上安装DoD证书链。检查 PKI POC,以获取证书/批处理文件。

下载 Cisco Anyconnect VPN 客户端 - Windows

1. 通过 Internet Explorer 启动与 ASA 的 Web 会话。地址格式应为:https://外部接口。例如 , https://172.18.120.225。

2. 选择要用于访问的签名证书。请参阅图 26。

图26:选择正确的证书

Choose a	digital certificate ation The Web site you want to identification. Please choo	o view requests ose a certificate.
	Name POOLE.JUSTIN.ALLE MCGINTY.JIMMY.11 POOLE.JUSTIN.ALLE MCGINTY.JIMMY.11	Issuer DOD CLASS 3 EMAIL CA-10 DOD JITC CA-15 DOD CLASS 3 CA-10 DOD JITC EMAIL CA-15
	Mo	re Info View Certificate OK Cancel

3. 当出现提示时,输入口令。

图27:输入PIN

ActivCa	ard Gold - Enter	PIN 🔀
	Enter PIN code:	
	ОК	Cancel

- 4. 选择 Yes 以接受安全警报。
- 5. 出现 SSL Login 页面后,选择 Login。使用客户端证书进行登录。请参阅图 28。

图28:SSL登录

jle Edit yew Fgyorites Iools Help	2
🔾 Back 🔹 🐑 😰 🐔 🔎 Search 👷 Favorites 🕢 🔗 🖓 📲 🔛 🏭 🖏	
ddress: 🍓 https://172.18.120.225/+CSCOE+/logon.html 😽 🖌	- 12
CISCO SSL VPN Service	
<u>i di si si</u>	

6. AnyConnect 开始下载客户端。请参阅图 29。

图29:安装AnyConnect



7. 选择要使用的相应证书。请参阅图 30。AnyConnect 继续安装。ASA 管理员可选择永久安装 客户端,或在每次 ASA 连接时安装。

图30:证书



启动 Cisco AnyConnect VPN 客户端 - Windows

从主机 PC 上选择"开始">"所有程序">"Cisco">"AnyConnect VPN 客户端"。

注意:有关可选AnyConnect客户端配置文件配置,请参阅附录E。

新建连接

1. 出现 AC 窗口。请参阅图 34。

图34:新VPN连接



2. 如果 AC 未自动进行连接,请选择相应主机。

3. 当出现提示时,输入口令。请参阅图 35。

图35:输入PIN

ActivCa	rd Gold - Enter	PIN 🔀
	Enter PIN code:	
	OK	Cancel

启动远程访问

选择要连接的组和主机。

因为使用证书,请选择 Connect 以建立 VPN。请参阅图 36。

图36:连接



注意:由于连接使用证书,因此无需输入用户名和密码。

注意:有关可选AnyConnect客户端配置文件配置,请参阅附录E。

附录 A - LDAP 映射和 DAP

在 ASA/PIX 版本 7.1(x) 和更高版本中,引入了一种被称作 LDAP 映射的功能。这项强大的功能提供 Cisco 属性与 LDAP 对象/属性之间的映射,因此无需更改 LDAP 架构。对于 CAC 身份验证实施,该功能可支持对远程访问连接实施其他策略。以下为 LDAP 映射的示例。请注意,如果要在 AD/LDAP 服务器中进行更改,您需要具备管理员权限。在ASA 8.x软件中,引入了动态访问策略 (DAP)功能。DAP 可结合 CAC,以用于查看多个 AD 组以及推送策略、ACL 等等。

方案1:使用远程访问权限拨入实施Active Directory -允许/拒绝访问

本示例将 AD 属性 msNPAllowDailin 映射到 Cisco 属性 cVPN3000-Tunneling- Protocol。

- AD属性值:TRUE =允许;FALSE =拒绝
- 思科属性值:1=FALSE、4 (IPSec)或20 (4 IPSEC + 16 WebVPN) = TRUE、

对于 ALLOW 情况,进行以下映射:

• TRUE = 20

对于 DENY 拨入情况,进行以下映射:

• FALSE = 1

注意:确保TRUE和FALSE全部大写。有关详细信息,请参阅<u>配置外部服务器以便进行安全设</u> <u>备用户授权。</u>

活动目录设置

- 1. 在 Active Directory 服务器中,单击 Start > Run。
- 2. 在 Open 文本框中, 键入 dsa.msc, 然后单击 Ok。这用来启动活动目录管理控制台。
- 3. 在 Active Directory 管理控制台中,请单击加号,展开 Active Directory Users and Computers。
- 4. 单击加号展开域名。
- 如果已为用户创建OU,请展开OU以查看所有用户;如果在"用户"文件夹中分配了所有用户 ,请展开该文件夹以查看所有用户。请参阅图 A1。

图A1:Active Directory管理控制台



6. 双击要编辑的用户。

单击用户属性页中的 Dial-in 选项卡,并单击 Allow 或 Deny。请参阅图 A2。

图A2:用户属性

1996 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 -		196 BA 96
Contraction of the second s	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	100.00

Environment Sessions Remo General Address Accou Published Certificates Men	nt Profile Terminal Services Profile COM+ nt Profile Telephones Organization nber Of Dial-in Object Security
Remote Access Permission (D C Allow access Deny access C Deny access C Control access through Re	ial-in or VPN) mote Access Bolicy
Callback Options Callback Options No Callback C Set by Caller (Routing and C Always Callback to:	Remote Access Service only)
Assign a Static IP Address Apply Static Boutes	
C Assign a Static IP Address	

7

7. 然后单击 OK。

ASA 配置

- 1. 在 ASDM 中,选择 Remote Access VPN> AAA Setup > LDAP Attribute Map。
- 2. 单击 Add。
- 3. 在 Add LDAP Attribute Map 窗口中,执行以下步骤。请参阅图 A3。

图A3:添加LDAP属性映射

🖆 Add LDAP Attribute Map				
Name: msNPAllowClain (1995) Map Name Map Value				
Customer Name: msNPAllowDialm	Add >>	Customer Name	Cisco Name	
	Cancel	Нар		

- a. 在"名称"文本框中输入名称。
- b. 在 Map Name 选项卡中,在 Customer Name 文本框中键入 msNPAllowDialin。
- c. 在 Map Name 选项卡中,从 Cisco Name 下拉选项中选择 Tunneling-Protocols。
- d. 单击 Add。
- e. 选择 Map Value 选项卡。
- f. 单击 Add。
- g. 在 Add Attribute LDAP Map Value 窗口中,在 Customer Name 文本框中键入 TRUE,并在 Cisco Value 文本框中键入 20。
- h. 单击 Add。
- i. 在 Customer Name 文本框中键入 FALSE,并在 Cisco Value 文本框中键入 1。请参阅 图 A4。

stomer Name: nsNPAllowOldin			
		Customer Value	Cisco Value
		FALSE	1
Customer Value:	Add >> << Remove		

- j. Click OK.
- k. Click OK.
- I. 单击 Apply。
- m. 配置结果如图 A5。
 - 图A5:LDAP属性映射配置

📬 Cisco ASDM 6.0 for ASA - 17.	2.18.120.225		
Ele View Tools Wigards Windo	w Help	Look For: Hot -	alulu
Home Configuration	fonitoring 🔚 Save 🌘	🗞 Refresh 😧 Back. 🥥 Forward 🧳 Help	CISCO
Remote Access V 🗗 🕈 🗡	Configuration > Rem	ote Access VPN > AAA Setup > LDAP Attribute Map	
Wetwork (Client) Access			
AAA Setup	Add and configure	attribute map used by LDAP server.	<u>, 10, 10</u>
AAA Server Groups			
Local Users	Name	Attribute Map Name	
🗟 🕂 Secure Desktop Manager 👱	msNPAlowDialn	ImsNPAllowDiain=Tunneling-Protocols	
			L
💑 Device Setup			
🕄 Firewall			
Remote Access VPN			
Site-to-Site VPN			
Device Management			
<u>и</u> •		Apply	

4. 选择 Remote Access VPN> AAA Setup > AAA Server Groups。请参阅图 A6。

图A6:AAA服务器组

📬 Cisco ASDM 6.0 for ASA - 17	2.18.120.225				
Ele Yew Tools Wigards Windo	w Help Yonitoring 🔛 Save (Look For:	Badk. 🚫 Forw	and 🧖 Help	cisco
Remote Access V 🗗 🕈 🗡	Configuration > Rea	ote Access VP	N > AAA Setup >	AAA Server Grou	ps 🗆
Access Network (Client) Access	AAA Server Groups				
AAA Setup	Server Group	Protocol	Accounting N	fode Reactiva	tion M Add
AAA Server Groups	AD-LDAP LOCAL	LDAP LOCAL		Depletion	Edit
🖶 🚮 Local Users 🖻 🕂 Secure Desktop Manager 👱	<	U.			> Delete
< <u> </u>	Servers in the Selected	Group			
A Device Setup	Server Name or IP	Address	Interface	Timeout	Add
Firewall	172.18.120.160		outside		10 Edit
Remote Access VPN					Delete
Site-to-Site VPN					Move Up
Device Management					(Move Down!!!)
÷			Apply R	eset	
Device configuration loaded	cis	00 15		3 🕟 🛛 🔀	7/17/07 1:59:07 PM UTC

- 5. 单击要编辑的服务器组。在 Selected Group 部分的 Servers 中,选择服务器 IP 地址或主机名 ,然后单击 Edit。
- 6. 在 Edit AAA Server 窗口中的 LDAP Attribute Map 文本框中,从下拉菜单中选择已创建的 LDAP 属性映射。请参阅图 A7。

图A7:添加LDAP属性映射

🖆 Edit AAA Server

Server Group:		AD-LDAP		
Interface Name:		outside	¥	
Server Name or IP Address:		172.18.120.160		
Timeout:		10		seconds
LDAP Parameters				
Enable LDAP over 1	SSL			
Server Port:	389			
Server Type:	De	etect Automatically/Use Generic Type		
Base DN:	CN=Users,DC=ggsgseclab,DC=org			
Scope:	One	lèvel beneath the Base DN		1

7. Click OK.

注意:在测试时打开LDAP调试,以验证LDAP绑定和属性映射是否正常工作。有关故障排除 命令,请参阅附录 C。

方案2:使用组成员身份允许/拒绝访问的Active Directory实施

本示例使用 LDAP 属性 memberOf 映射到 Tunneling Protocol 属性,以便建立作为条件的组成员。

为使此策略生效,必须具备以下条件:

- 针对 ALLOW 情况,使用现有组,或是创建一个新组并将 ASA VPN 用户添加到新组中。
- 针对 DENY 情况,使用现有组,或是创建一个新组并将非 ASA 用户添加到新组中。
- 确保在 LDAP 查看器中检查该组是否具备正确的 DN。请参阅附录 D。如果 DN 错误,映射将 无法正常运行。

注意:请注意,在此版本中,ASA只能读取memberOf属性的第一个字符串。确保新创建的组 位于列表顶端。或者,在名称前插入一个特殊字符,因为 AD 会首先查看特殊字符。要处理此 警告,请在 8.x 软件中使用 DAP 来查看多个组。

注意:确保用户是拒绝组或至少一个其他组的一部分,以便memberOf始终发送回ASA。虽然 不是必需操作,但建议您指定 FALSE 拒绝条件。如果现有组名称包含空格,请按照以下方式 输入属性:

CN=Backup Operators, CN=Builtin, DC=ggsgseclab, DC=org

注意:DAP允许ASA在memberOf属性中查看多个组,并对组进行基本授权。请参阅 DAP 部 分。

映射

- AD 属性值:
 - memberOf CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
 - memberOf CN=TelnetClients, Cn=users, DC=labrat, Dc=com
- Cisco属性值:1=FALSE,20=TRUE,

对于 ALLOW 情况,进行以下映射:

memberOf CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org= 20

对于 DENY 情况,进行以下映射:

memberOf CN=TelnetClients,CN=Users,DC=ggsgseclab,DC=org = 1

注意:在将来的版本中,有一个Cisco属性用于允许和拒绝连接。有关 Cisco 属性的详细信息 ,请参阅<u>配置外部服务器以便进行安全设备用户授权。</u>

活动目录设置

1. 在 Active Directory 服务器中,单击 Start > Run。

- 2. 在 Open 文本框中,键入 dsa.msc, 然后单击 Ok。这用来启动活动目录管理控制台。
- 3. 在 Active Directory 管理控制台中,请单击加号,展开 Active Directory Users and Computers。请参阅图 A8。
 - 图A8:Active Directory组

jele Action yew Window He ⊨ → 💽 💽 👗 🗙 🛠 🛱 🗔	⊳ \$\ 00 \$≈766	;		<u>_10 </u> >
Active Directory Users and Computer	Users 23 objects			
E 📄 Saved Queries	Name	Туре	Description	1
🖹 🚺 labrat.com	2 Administrator	User	Buik-in account for administering the co	
🕀 🤐 Buikin	2 artperez	User		
Computers	ASALIsers	Security Group	VPN Remote Access Users	0.000
Onnain Controlers	Cert Publishers	Security Group	Members of this group are permitted to	
PoreignsecuncyPrincipas	CERTSVC_DCOM_ACCESS	Security Group		
California (2 DnsAdmins	Security Group	DNS Administrators Group	
	2 DnsUpdateProxy	Security Group	DNS clients who are permitted to perfor	
	Domain Admins	Security Group	Designated administrators of the domain	
	Domain Computers	Security Group	All workstations and servers joined to th	
	Domain Controllers	Security Group	All domain controllers in the domain	
	Domain Guests	Security Group	All domain guests	
	Domain Users	Security Group	All domain users	
	DEnterprise Admins	Security Group	Designated administrators of the enterp	
	Group Policy Creator Owners	Security Group	Members in this group can modify group	
	Guest	User	Built-in account for guest access to the	
	1 HelpServicesGroup	Security Group	Group for the Help and Support Center	
	TII5_WPG	Security Group	IIS Worker Process Group	
	IUSR_CISCOJAX-2K3	User	Built-in account for anonymous access t	
	IWAM_CISCOJAX-2K3	User	Built-in account for Internet Information	
	RAS and IAS Servers	Security Group	Servers in this group can access remote	
	Schema Admins	Security Group	Designated administrators of the schema	
	50 SUPPORT_388945a0	User	This is a vendor's account for the Help a	
Include the second s	TeinetClients	Security Group	Members of this group have access to T	- (+ (+ (+ (+

- 4. 单击加号展开域名。
- 5. 右键单击 Users 文件夹,并选择 New > Group。
- 6. 输入组名称。例如:ASAUsers。
- 7. Click OK.
- 8. 单击 Users 文件夹,然后双击刚创建的组。
- 9. 选择 Members 选项卡, 然后单击 Add。
- 10. 键入要添加的用户的 Name, 然后单击 Ok。

ASA 配置

- 1. 在 ASDM 中,选择 Remote Access VPN> AAA Setup > LDAP Attribute Map。
- 2. 单击 Add。

- 3. 在 Add LDAP Attribute Map 窗口中,执行以下步骤。请参阅图 A3。
 - a. 在"名称"文本框中输入名称。
 - b. 在 Map Name 选项卡中,在 Customer Name 文本框 c 中键入 memberOf。
 - c. 在 Map Name 选项卡中,从 Cisco Name 下拉选项中选择 Tunneling-Protocols。
 - d. 选择 Add。
 - e. 单击 Map Value 选项卡。
 - f. 选择 Add。
 - g. 在 Add Attribute LDAP Map Value 窗口中,在 Customer Name 文本框中键入 CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org,并在 Cisco Value 文本框中键入 20。
 - h. 单击 Add。
 - i. 在 Customer Name 文本框中键入 CN=TelnetClients,CN=Users,DC=ggsgseclab,DC=org,并在 Cisco Value 文本框中键 入1。请参阅图 A4。
 - j. Click OK.
 - k. Click OK.
 - I. 单击 Apply。
 - m. 配置结果如图 A9。
 - 图 A9 LDAP 属性映射

Cisco ASDM 6.0 for ASA - 172	.18.120.225		
Ele Yew Tools Wigards Window	v Help onitoring 📊 Save (Look For:	Find It is the image of the
Remote Access V Network (Client) Access Clientless SSL VPN Access AAA Setup AAA Server Groups	Configuration > Rer Add and configure	note Access VPN > AAA Setup > LDA attribute map used by LDAP server.	P Attribute Map 🛛
Cocal Users Cocal Users Coca	Name memberOf	Attribute Map Name memberOf—Tunneling-Protocols	
Erewall Ere			
Device Management		Apply Reset	

- 4. 选择 Remote Access VPN> AAA Setup > AAA Server Groups。
- 5. 单击要编辑的服务器组。在 Selected Group 部分的 Servers 中,选择服务器 IP 地址或主机名 , 然后单击 Edit。

Name: memberOf		
ap Name Map Value		
Customer Name	Customer to Gisco Map Value	Add
memberOf	CN=TelnetClients, CN=Users, DC=ggsgsedab, DC=org=1 CN=ASAUsers, CN=Users, DC=associab, DC=aso=20	
		Edt in i
		Delete
		 - • • • • • • • • • • • • • • • • • • •

6. 在 Edit AAA Server 窗口中的 LDAP Attribute Map 文本框中,从下拉菜单中选择已创建的 LDAP 属性映射。

注意:请在测试时打开LDAP调试,以验证LDAP绑定和属性映射是否正常工作。有关故障排 除命令,请参阅附录 C。

场景3:多个memberOf属性的动态访问策略

本示例使用 DAP 查看多个 memberOf 属性。在 8.x 版本之前,ASA 仅读取第一个 memberOf 属性。在 8.x 版本和更高版本中,ASA 可查看所有 memberOf 属性。

- 针对 ALLOW 情况,使用现有组,或是新建一个组(或多个组)并将 ASA VPN 用户添加到新 组中。
- 针对 DENY 情况,使用现有组,或是创建一个新组并将非 ASA 用户添加到新组中。
- 确保在 LDAP 查看器中检查该组是否具备正确的 DN。请参阅附录 D。如果 DN 错误,映射将 无法正常运行。

ASA 配置

- 1. 在 ASDM 中,选择 Remote Access VPN> Network (Client) Access > Dynamic Access Policies。
- 2. 单击 Add。
- 3. 在 Add Dynamic Access Policy 中,执行以下步骤:
 - a. 在 Name 文本框 b 中输入名称。
 - b. 在 Priority 部分, 输入1或者大于0的其他数字。
 - c. 在 Selection Criteria 中,单击 Add。
 - d. 在 Add AAA Attribute 中,选择 LDAP。
 - e. 在 attribute ID 部分中, 输入 memberOf。
 - f. 在 value 部分中,选择 = 并输入 AD 组名。针对要引用的每个组重复此步骤。请参阅图 A10。

图 A10 AAA 属性映射

🚰 Add AAA	Attribute 🔀
AAA Attribute	• Type: LDAP
Attribute ID:	memberOf
Value:	

- g. Click OK.
- h. 在 Access Policy Attributes 部分中,选择 Continue。请参阅图 A11。
 - 图 A11 添加动态策略

	CMC-UDERS				
escription:	Multi-Group Membership Check			Priority: 1	
Selection O	tera				
Define the below and specify th	 AAA and endpoint attributes used to select this access devery endpoint attribute has been satisfied. These at a logical expression text. 	ss policy. A policy i tributes can be or	s used when a user's i eated using the tables	authorization attributes match the AJ below and/or by expanding the Adv	AA attribute oriteria anced option to
User has	ANY of the following AAA Attributes values 🛛 😽		and the following en	dpoint attributes are satisfied.	
MA AAA	vibute Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
Idap.mem	berOf = _ASALIsers	Edit			Edit
luap.men	Deror = YPYUsers				
		Delete			Desce
					Logical Op.
Advanc	red				3
Advance Access Polic Configure Action	ed y Attributes access policy attributes for this policy. Attributes valu Network ACL Filters Web-Type ACL Filters Function	es specified here i Is Port Forwardi	uli override those valu	ies obtained from the AAA system. ccess Method	*
Advance Access Pole Configure Action Action	ed access policy attributes for this policy. Attributes valu Network ACL Filters Web-Type ACL Filters Function © Continue Terminate	es specified here i Is Port Forwardi	vill override those valu ng Lists URL Lists A	ies obtained from the AAA system. ccess Method	•
Advanc Access Pole Configure Action Action Specify	ed access policy attributes for the policy. Attributes valu Network ACL Filters Web-Type ACL Filters Function © Continue O Terminate the message that will be displayed when this record is	es specified here v Is Port Forwardi selected.	vill override those valu ng Lists URL Lists A	ies obtained from the AAA system. ccess Method	•
Advanc Configure Action Action Specify User M	eed cy Attributes access policy attributes for this policy. Attributes valu Network ACL Filters Web-Type ACL Filters Function Continue Continue the message that will be displayed when this record is essage:	es specified here a Is Port Forwardi selected.	vil override those valu Ig Lists URL Lists A	ies obtained from the AAA system. ccess Method	•

- 4. 在 ASDM 中,选择 Remote Access VPN> Network (Client) Access > Dynamic Access Policies。
- 5. 选择 Default Access Policy,并选择 Edit。
- 6. 默认操作应设为 Terminate。请参阅图 A12。

图 A12 编辑动态策略

Description: Access Policy Attributes Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA syst Action Network ACL Filters Web-Type ACL Filters Functions Port Forwarding Lists URL Lists Access Method Action: O Continue O Terminate Specify the message that will be displayed when this record is selected.		DftAccessPolicy
Access Policy Attributes Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA syst Action Network ACL Filters Web-Type ACL Filters Functions Port Forwarding Lists URL Lists Access Method Action: Continue Terminate Specify the message that will be displayed when this record is selected.	Description:	
Action Network ACL Filters Web-Type ACL Filters Functions Port Forwarding Lists URL Lists Access Method Action: O Continue Image: Terminate Image: Terminate Image: Terminate Image: Terminate Specify the message that will be displayed when this record is selected. Image: Terminate Image: Terminate Image: Terminate	Access Pol	cy Attributes e access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.
Action: O Continue O Terminate Specify the message that will be displayed when this record is selected.	Action	Network ACL Filters Web-Type ACL Filters Functions Port Forwarding Lists URL Lists Access Method
	Specif	the message that will be displayed when this record is selected.
User Message:		
	User M	essage:

注意:如果未选择Terminate,您将无法进入任何组,因为默认值为Continue。

附录 B - ASA CLI 配置

ASA 5510 <#root> ciscoasa# show running-config : Saved ASA Version 8.0(2) hostname asa80 domain-name army.mil enable password 8Ry2YjIyt7RRXU24 encrypted names interface GigabitEthernet0/0 nameif outside security-level 0 ip address x.x.x.x 255.255.255.128 interface GigabitEthernet0/1 nameif inside security-level 100 no ip address boot system disk0:/asa802-k8.bin ftp mode passive dns server-group DefaultDNS domain-name army.mil -----ACL's----access-list out extended permit ip any any _____ _____ pager lines 24 logging console debugging mtu outside 1500 -----VPN Pool------ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask 255.255.255.0 _____ no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400 access-group out in interface outside route outside 0.0.0.0 0.0.0.0 172.18.120.129 1 timeout xlate 3:00:00

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout uauth 0:05:00 absolute
 -----LDAP Maps & DAP-----
ldap attribute-map memberOf
map-name memberOf Tunneling-Protocols
March 11, 2008 ASA - CAC Authentication for AnyConnect VPN Access
Company Confidential. A printed copy of this document is considered uncontrolled.
49
map-value memberOf CN=_ASAUsers,CN=Users,DC=ggsgseclab,DC=org 20
ldap attribute-map msNPAllowDialin
map-name msNPAllowDialin Tunneling-Protocols
map-value msNPAllowDialin FALSE 1
map-value msNPAllowDialin TRUE 20
dynamic-access-policy-record CAC-USERS
description "Multi-Group Membership Check"
priority 1
dynamic-access-policy-record DfltAccessPolicy
action terminate
-----LDAP Server-----
aaa-server AD-LDAP protocol ldap
aaa-server AD-LDAP (outside) host 172.18.120.160
ldap-base-dn CN=Users,DC=ggsgseclab,DC=org
ldap-scope onelevel
ldap-naming-attribute userPrincipalName
ldap-login-password *
ldap-login-dn CN=Administrator,CN=Users,DC=ggsgseclab,DC=org
aaa authentication http console LOCAL
http server enable 445
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
   -----CA Trustpoints-----
crypto ca trustpoint ASDM_TrustPoint0
revocation-check ocsp
enrollment terminal
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
crl configure
crypto ca trustpoint ASDM_TrustPoint1
revocation-check ocsp
enrollment terminal
fqdn asa80
subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S. Government,C=US
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint2
revocation-check ocsp
```

enrollment terminal keypair DoD-2048 match certificate DefaultCertificateMap override ocsp trustpoint ASDM_TrustPoint5 10 url http://ocsp.disa.mil no client-types crl configure crypto ca trustpoint ASDM_TrustPoint3 revocation-check ocsp none enrollment terminal crl configure ----- Certificate Map-----crypto ca certificate map DefaultCertificateMap 10 subject-name ne "" ------CA Certificates (Partial Cert is Shown)-----crypto ca certificate chain ASDM_TrustPoint0 certificate ca 37 3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101 05050030 60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53 2e20476f 7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603 55040b13 03504b49 311b3019 06035504 03131244 6f44204a 49544320 526f6f74 crypto ca certificate chain ASDM_TrustPoint1 certificate 319e 30820411 3082037a a0030201 02020231 9e300d06 092a8648 86f70d01 01050500 305c310b 30090603 55040613 02555331 18301606 0355040a 130f552e 532e2047 6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b crypto ca certificate chain ASDM_TrustPoint2 certificate ca 37 3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101 05050030 60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53 2e20476f 7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603 55040b13 f766e045 f15ddb43 9549d1e9 a0ea6814 b64bcece 089e1b6e 1be959a5 6fc20a76 crypto ca certificate chain ASDM_TrustPoint3 certificate ca 05 30820370 30820258 a0030201 02020105 300d0609 2a864886 f70d0101 05050030 5b310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53 2e20476f 7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603 55040b13 03504b49 31163014 06035504 03130d44 6f442052 6f6f7420 43412032 301e170d 30343132 31333135 30303130 5a170d32 39313230 35313530 3031305a 305b310b 30090603 55040613 02555331 18301606 0355040a 130f552e 532e2047 6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b 1303504b 49311630 14060355 0403130d 446f4420 526f6f74 20434120 32308201 crypto ca certificate chain ASDM_TrustPoint4 certificate ca 04 30820267 308201d0 a0030201 02020104 300d0609 2a864886 f70d0101

```
05050030
61310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 311c301a 06035504 03131344 6f442043 4c415353 20332052
6f6f7420
class-map inspection_default
match default-inspection-traffic
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
service-policy global_policy global
    -----windows-----SSL/WEBvpn-windows------
ssl certificate-authentication interface outside port 443
webvpn
enable outside
svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
svc enable
tunnel-group-list enable
        -----PN Group/Tunnel Policy------
group-policy CAC-USERS internal
ggroup-policy AC-USERS internal
group-policy AC-USERS attributes
vpn-windows-tunnel-protocol svc
address-pools value CAC-USERS
webvpn
svc ask none default svc
tunnel-group AC-USERS type remote-access
tunnel-group AC-USERS general-attributes
authorization-server-group AD-LDAP
default-group-policy AC-USERS
authorization-required
authorization-dn-attributes UPN
tunnel-group AC-USERS webvpn-windows-attributes
authentication certificate
group-alias AC-USERS enable
tunnel-group-map enable rules
no tunnel-group-map enable ou
```

```
no tunnel-group-map enable ike-id
no tunnel-group-map enable peer-ip
```

prompt hostname context

附录 C - 故障排除

AAA 和 LDAP 故障排除

- debug Idap 255 显示 LDAP 交换
- debug aaa common 10 显示 AAA 交换

示例1:具有正确属性映射的允许连接

本示例显示在与附录 A 中场景 2 的成功连接期间 debug ldap 和 debug aaa common 的输出。

图C1:debug LDAP和debug aaa common输出-正确的映射 AAA API: In aaa_open AAA session opened: handle = 39 AAA API: In aaa_process_async aaa_process_async: sending AAA_MSG_PROCESS AAA task: aaa_process_msg(1a87a64) received message type 0 AAA FSM: In AAA_StartAAATransaction AAA FSM: In AAA_InitTransaction Initiating authorization query (Svr Grp: AD-LDAP) _____ AAA FSM: In AAA_BindServer AAA_BindServer: Using server: 172.18.120.160 AAA FSM: In AAA_SendMsg User: 1234567890@mil Pasw: 1234567890@mil Resp: [78] Session Start [78] New request Session, context 0x26f1c44, reqType = 0 [78] Fiber started [78] Creating LDAP context with uri=ldap:// 172.18.120.160:389 [78] Binding as administrator [78] Performing Simple authentication for Administrator to 172.18.120.160 [78] Connect to LDAP server: ldap:// 172.18.120.160, status = Successful [78] LDAP Search: Base DN = [CN=Users,DC=ggsgseclab,DC=org] Filter = [userPrincipalName=1234567890@mil] Scope = [SUBTREE][78] Retrieved Attributes: [78] objectClass: value = top [78] objectClass: value = person [78] objectClass: value = organizationalPerson [78] objectClass: value = user [78] cn: value = Ethan Hunt

```
[78] sn: value = Hunt
[78] userCertificate: value =
0..50....../.....60....*.H.....0@1.0.....&...,d....com1.0.....
&...,d...
[78] userCertificate: value =
0...'0....../..t.....50...*.H......0@1.0....&...,d....com1.0.....
&...,d...
[78] givenName: value = Ethan
[78] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[78] instanceType: value = 4
[78] whenCreated: value = 20060613151033.0Z
[78] whenChanged: value = 20060622185924.0Z
[78] displayName: value = Ethan Hunt
[78] uSNCreated: value = 14050
[78] memberOf: value = CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[78] mapped to cVPN3000-Tunneling-Protocols: value = 20
[78] uSNChanged: value = 14855
[78] name: value = Ethan Hunt
[78] objectGUID: value = ..9...NJ..GU..z.
[78] userAccountControl: value = 66048
[78] badPwdCount: value = 0
[78] codePage: value = 0
[78] countryCode: value = 0
[78] badPasswordTime: value = 127954717631875000
[78] lastLogoff: value = 0
[78] lastLogon: value = 127954849209218750
[78] pwdLastSet: value = 127946850340781250
[78] primaryGroupID: value = 513
[78] objectSid: value = .....q.....q.....mY...
[78] accountExpires: value = 9223372036854775807
[78] logonCount: value = 25
[78] sAMAccountName: value = 1234567890
[78] sAMAccountType: value = 805306368
[78] userPrincipalName: value = 1234567890@mil
[78] objectCategory: value =
[78] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
[78] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[78] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
 _____
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(CAC-USERS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
    AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USER
Pasw:
```

Resp: grp_policy_ioctl(12f1b20, 114698, 1a870b4) grp_policy_ioctl: Looking up CAC-USERS callback_aaa_task: status = 1, msg = AAA FSM: In aaa_backend_callback aaa_backend_callback: Handle = 39, pAcb = 2ae115c AAA task: aaa_process_msg(1a87a64) received message type 1 AAA FSM: In AAA_ProcSvrResp Back End response: _____ Tunnel Group Policy Status: 1 (ACCEPT) AAA FSM: In AAA_NextFunction AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status = ACCEPT AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol = , tunn pol = CAC-USERS AAA_NextFunction: New i_fsm_state = IFSM_DONE, AAA FSM: In AAA_ProcessFinal Checking time simultaneous login restriction for user 1234567890@mil AAA FSM: In AAA_Callback user attributes: 1 Tunnelling-Protocol(4107) 20 20 user policy attributes: None tunnel policy attributes: 1 Primary-DNS(4101) 4 IP: 10.0.10.100 2 Secondary-DNS(4102) 4 IP: 0.0.0.0 3 Tunnelling-Protocol(4107) 4 4 4 Default-Domain-Name(4124) 10 "ggsgseclab.org" 5 List of address pools to assign addresses from(4313) 10 "CAC-USERS" Auth Status = ACCEPT AAA API: In aaa_close AAA task: aaa_process_msg(1a87a64) received message type 3 In aaai_close_session (39) AAA API: In aaa_send_acct_start AAA API: In aaa_send_acct_stop CAC-Test#

示例2:思科属性映射配置错误的允许连接

本示例显示在与附录 A 中场景 2 的允许连接期间 debug ldap 和 debug aaa common 的输出。

```
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[82] Session Start
[82] New request Session, context 0x26f1c44, reqType = 0
[82] Fiber started
[82] Creating LDAP context with uri=ldap://172.18.120.160:389
[82] Binding as administrator
[82] Performing Simple authentication for Administrator to
172.18.120.160
[82] Connect to LDAP server: ldap:// 172.18.120.160:389, status =
Successful
[82] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[82] Retrieved Attributes:
[82] objectClass: value = top
[82] objectClass: value = person
[82] objectClass: value = organizationalPerson
[82] objectClass: value = user
[82] cn: value = Ethan Hunt
[82] sn: value = Hunt
[82] userCertificate: value =
0...50....../..../......60....*.H......0@1.0.....&...,d....com1.0....
&...,d...
[82] userCertificate: value =
0...'0......./..t.....50....*.H......0@1.0.....&...,d....com1.0....
&...,d...
[82] givenName: value = Ethan
[82] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[82] instanceType: value = 4
[82] whenCreated: value = 20060613151033.0Z
[82] whenChanged: value = 20060622185924.0Z
[82] displayName: value = Ethan Hunt
[82] uSNCreated: value = 14050
[82] memberOf: value = CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers, CN=Users, DC=ggsgseclab, DC=org
[82] uSNChanged: value = 14855
[82] name: value = Ethan Hunt
[82] objectGUID: value = ..9...NJ..GU..z.
[82] userAccountControl: value = 66048
[82] badPwdCount: value = 0
[82] codePage: value = 0
[82] countryCode: value = 0
[82] badPasswordTime: value = 127954717631875000
[82] lastLogoff: value = 0
[82] lastLogon: value = 127954849209218750
[82] pwdLastSet: value = 127946850340781250
[82] primaryGroupID: value = 513
[82] objectSid: value = .....q.....q.....
[82] accountExpires: value = 9223372036854775807
[82] logonCount: value = 25
[82] sAMAccountName: value = 1234567890
[82] sAMAccountType: value = 805306368
[82] userPrincipalName: value = 1234567890@mil
[82] objectCategory: value =
CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=org
[82] mail: value = Ethan.Hunt@labrat.com
```

callback_aaa_task: status = 1, msg = AAA FSM: In aaa_backend_callback aaa_backend_callback: Handle = 41, pAcb = 2ae115c [82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1 [82] Session End AAA task: aaa_process_msg(1a87a64) received message type 1 AAA FSM: In AAA_ProcSvrResp Back End response: _____ Authorization Status: 1 (ACCEPT) AAA FSM: In AAA_NextFunction AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol = , tunn pol = CAC-USERSAAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY, AAA FSM: In AAA_InitTransaction aaai_policy_name_to_server_id(USAFE) Got server ID 0 for group policy DB Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB) AAA FSM: In AAA_BindServer AAA_BindServer: Using server: <Internal Server> AAA FSM: In AAA_SendMsg User: CAC-USERS Pasw: Resp: grp_policy_ioctl(12f1b20, 114698, 1a870b4) grp_policy_ioctl: Looking up CAC-USERS callback_aaa_task: status = 1, msg = AAA FSM: In aaa_backend_callback aaa_backend_callback: Handle = 41, pAcb = 2ae115c AAA task: aaa_process_msg(1a87a64) received message type 1 AAA FSM: In AAA_ProcSvrResp Back End response: Tunnel Group Policy Status: 1 (ACCEPT) AAA FSM: In AAA_NextFunction AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status = ACCEPT AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol = , tunn pol = CAC-USERS AAA_NextFunction: New i_fsm_state = IFSM_DONE, AAA FSM: In AAA_ProcessFinal Checking time simultaneous login restriction for user 1234567890@mil AAA FSM: In AAA_Callback user attributes: 1 Tunnelling-Protocol(4107) 20 0 user policy attributes: None tunnel policy attributes: 1 Primary-DNS(4101) 4 IP: 10.0.10.100 2 Secondary-DNS(4102) 4 IP: 0.0.0.0 3 Tunnelling-Protocol(4107) 4 4 4 Default-Domain-Name(4124) 10 "ggsgseclab.org" 5 List of address pools to assign addresses from(4313) 10 "CAC-USERS" Auth Status = ACCEPT AAA API: In aaa_close AAA task: aaa_process_msg(1a87a64) received message type 3 In aaai_close_session (41) AAA API: In aaa_send_acct_start AAA API: In aaa_send_acct_stop

DAP 故障排除

- debug dap errors 显示 DAP 错误
- debug dap trace 显示 DAP 功能跟踪

示例1:允许与DAP的连接

本示例显示在与附录A中所示场景3的成功连接期间debug dap errors和debug dap trace的输出。注 意多个memberOf属性。您可同时属于 _ASAUsers 和 Vpnuser 组,或属于任何一个组,这取决于 ASA 配置。

图C3:debug DAP <#root> debug dap errors debug dap errors enabled at level 1 debug dap trace debug dap trace enabled at level 1 The DAP policy contains the following attributes for user: 1241879298@mil 1: action = continue DAP_TRACE: DAP_open: C8EEFA10 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 = organizationalPerson DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.physicalDeliveryOfficeName = NETADMIN DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName = CN=1241879298, CN=Users, DC=ggsgseclab, DC=org DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated = 20070626163734.0Z DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged = 20070718151143.0Z DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.1 = VPNUsers DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2 = _ASAUsers DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
....+..F.."5....
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ...
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298, CN=Users, DC=ggsgseclab, DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] =
"VPNUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
"_ASAUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
```

```
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] = "CACUSERS"
DAP_TRACE: dap_add_to_lua_tree:endpoint["application"]["clienttype"] =
"IPSec";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs: CAC-USERS
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
DAP_TRACE: Username: 1241879298@mil, DAP_close: C8EEFA10
d.
```

示例2:与DAP的连接被拒绝

本示例显示在与附录 A 中所示场景 3 的未成功连接期间 debug dap errors 和 debug dap trace 的输 出。

图C4:debug DAP	
<#root>	
#	
debug dap errors	
debug dap errors enabled at level 1 #	
debug dap trace	

debug dap trace enabled at level 1 The DAP policy contains the following attributes for user: 1241879298@mil 1: action = terminate DAP_TRACE: DAP_open: C91154E8 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 = organizationalPerson DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.physicalDeliveryOfficeName = NETADMIN DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName = CN=1241879298, CN=Users, DC=ggsgseclab, DC=org DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated = 20070626163734.0Z DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged = 20070718151143.0Z DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf = DnsAdmins DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =+..F.."5.... DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl = 328192 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet = 128273494546718750 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m: d. DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ... DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires = 9223372036854775807 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName = 1241879298 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType = 805306368 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName = 1241879298@mil DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory = CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=org DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username = 1241879298@mil DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top"

```
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
 'person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298, CN=Users, DC=ggsgseclab, DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] = "DnsAdmins";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs:
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 0 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
```

故障排除认证中心/OCSP

- · debug crypto ca 3
- 在配置模式下 记录 class ca 控制台(或缓冲区)调试

以下示例显示了一次使用 OCSP Responder 成功进行的证书验证,以及一个错误的证书组匹配策略 。

图C3显示了包含已验证证书和工作证书组匹配策略的调试输出。

图 C4 显示了一个配置错误的证书组匹配策略的调试输出。

图 C5 显示了具有已撤销证书的用户的调试输出。

图C5:OCSP调试-成功的证书验证

CRYPTO_PKI: Found a suitable authenticated trustpoint ASDM_TrustPoint11. CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8 CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting to retrieve revocation status if necessary CRYPTO_PKI: status = 0: poll revocation status CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial number: OF192B, subject name: cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S. Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-15,ou=PKI,ou=DoD,o=U.S. Government,c=US. CRYPTO_PKI: Processing map rules for SSL. CRYPTO_PKI: Processing map SSL sequence 20... CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field: = cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S. Government,c=US, map rule: subject-name ne "". CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20. CRYPTO_PKI: Found OCSP override match. Override URL: http://198.154.68.90, Override trustpoint: ASDM_TrustPoint12 CRYPTO_PKI: crypto_pki_get_cert_record_by_subject() CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8 Crypto CA thread sleeps! CRYPTO_PKI: Attempting to find tunnel group for cert with serial number: OF192B, subject name: cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S. Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-15,ou=PKI,ou=DoD,o=U.S. Government,c=US. CRYPTO_PKI: Processing map rules for DefaultCertificateMap. CRYPTO_PKI: Processing map DefaultCertificateMap sequence 10... CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field: = cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S. Government,c=US, map rule: subject-name ne "". CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap sequence: 10. CRYPTO_PKI: Ignoring match on map DefaultCertificateMap, index 10 for WebVPN group map processing. No tunnel group is configured. CRYPTO_PKI: Peer cert could not be authorized with map: DefaultCertificateMap. CRYPTO_PKI: Processing map rules for SSL.

CRYPTO_PKI: Processing map SSL sequence 20... CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field: = cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S. Government,c=US, map rule: subject-name ne "". CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20. CRYPTO_PKI: Ignoring match on map SSL, index 20 for WebVPN group map

图C5:失败的证书组匹配策略的输出

图C5:已撤销证书的输出 n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled uvalidation=. CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,valdid cor =noct oamuthori,zed. map rule: subject-name ne "". CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap sequence: 10. Tunnel Group Match on map DefaultCertificateMap sequence # 10. Group name is CAC-USERS CRYPTO_PKI: Checking to see if an identical cert is already in the database... CRYPTO_PKI: looking for cert in handle=2467668, digest= CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND CRYPTO_PKI: Cert not found in database. CRYPTO_PKI: Looking for suitable trustpoints... CRYPTO_PKI: Found a suitable authenticated trustpoint trustpoint0. CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting to retrieve revocation status if necessary CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial number: 2FB5FC7400000000035, subject name: cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org, issuer_name: cn=ggsgseclab,dc=ggsgseclab,dc=org. CRYPTO_PKI: Processing map rules for DefaultCertificateMap. CRYPTO_PKI: Processing map DefaultCertificateMap sequence 10... CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field: = cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org, map rule: subject-name ne "". CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap sequence: 10. CRYPTO_PKI: Found OCSP override match. Override URL: http://ocsp.disa.mil, Override trustpoint: OCSP CRYPTO_PKI: crypto_pki_get_cert_record_by_subject() CRYPTO_PKI: Found a subject match ERROR: Certificate validation failed, Certificate is revoked, serial number: 2FB5FC7400000000035, subject name: cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org CRYPTO PKI: Certificate not validated

附录 D - 在 MS 中验证 LDAP 对象

在 Microsoft server 2003 CD 中提供了其他一些可供安装的工具,您可以使用这些工具来查看 LDAP 结构和 LDAP 对象/属性。要安装这些工具,请选择 CD 中的 Support 目录,然后选择

Tools。安装 SUPTOOLS.MSI。

LDAP 查看器

- 1. 完成安装后,请选择 Start > Run。
- 2. 键入 ldp,然后单击 Ok。这将启动 LDAP 查看器。
- 3. 选择 Connection > Connect。
- 4. 输入服务器名,然后单击 Ok。
- 5. 选择 Connection > Bind。
- 6. 输入用户名和密码。

注意:您需要管理员权限。

- 7. Click OK.
- 8. 查看 LDAP 对象。请参阅图 D1。

图D1:LDAP查看器

kap://Ciscojax-2k3.labrat.com/DC=labrat,DC=com	28 X
Connection Browse Yew Options Utilities	Bec
DC-labrat, DC-wom CN+eGunputers, DC-wom CN+eGunputers, DC-wom CN+eGunputers, DC-wom CN+eGunputers, DC-wabrat, DC-wom CN+eInfrastructure, DC-wabrat, DC-wom CN+EInfrastruc	Expanding base 'CN=Clark Kent,OU=MIL,DC=labrat,DC=com' Result (D): [null] Matched DNs: Getting 1 entries: >> Dn: CN=Clark Kent,OU=MIL,DC=labrat,DC=com

活动目录服务接口编辑器

- 在 Active Directory 服务器中,单击 Start > Run。
- 键入 adsiedit.msc。这将启动编辑器。
- 右键单击对象,并单击 Properties。

此工具将显示特定对象的所有属性。请参阅图 D2。

图D2:ADSI编辑

ADSI Edit Domain [Ciscojax-2k3.lal	Attribute Editor Security	nutes es		stow in t	Distinguished Name
CN=Computers OU=Domain Cor	F Show only attributes If Attributes:	hat have <u>y</u> alues			
CN=Corregrised CN=LostAndFou CN=CostAndFou CN=Clark Ke CN=Pthan H CN=Pthan H CN=Pter Pt CN=Ptogram Da CN=System CN=Users Configuration [Ciscojax- Schema [Ciscojax-2k3.la CN=Ethan Hunt [Ciscoja	Attribute unicodePvid url userCent userCent/icate userParameters userPassword userPKCS12 UserPhropoName userSharedFolder userSharedFolder userShiMECentricate userWorkstations 4 Edit	Syntax Octet String Unicode String Integer Octet String Octet String Octet String Octet String Unicode String Unicode String Unicode String Unicode String Unicode String	Value Chot Seb Chot Seb 66048 Chot Seb 0x30 0x82 0x06 0x27 0x3 mc dl Chot Seb Chot Seb Chot Seb Chot Seb Chot Seb Chot Seb Chot Seb Chot Seb		
		ОК	Cancel App		

附录 E

您可以创建一个 AnyConnect 配置文件,并将其添加到工作站。此配置文件可引用各种值(如 ASA 主机)或证书匹配参数(如识别名或颁发者)。此配置文件将存储为 .xml 文件,且可通过 Notepad 进行编辑。您可手动将该文件添加到每个客户端,或者通过组策略将其从 ASA 中推入客户端。文件 存储在:

 $\label{eq:locuments} C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile$

请完成以下步骤:

- 1. 选择 AnyConnectProfile.tmpl,并使用 Notepad 打开该文件。
- 2. 对该文件进行相应修改,如修改颁发者或主机 IP。有关示例,请参阅图 F1。
- 3. 完成后,以.xml 格式保存文件。

有关配置文件管理,请参阅 Cisco AnyConnect 文档。简而言之:

- 配置文件必须以公司名唯一命名。例如: CiscoProfile.xml
- 配置文件名称必须相同,即使在公司内部的各个组之间有所不同。

此文件由 Secure Gateway 管理员维护,并通过客户端软件分发。基于此 XML 的配置文件可随时分 发到各客户端。支持的分发机制有:随软件捆绑分发,或作为自动下载机制的一部分。自动下载机 制仅适用于某些 Cisco 安全网关产品。

注意:强烈建议管理员使用在线验证工具或通过ASDM中的配置文件导入功能验证他们创建的 XML配置文件。可借助本目录中的 AnyConnectProfile.xsd 完成验证。AnyConnectProfile 是 代表 AnyConnect 客户端配置文件的根元素。

这是 Cisco AnyConnect VPN 客户端配置文件 XML 文件的一个示例。

<#root> xml version="1.0" encoding="UTF-8" - - <AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd"> !--- The ClientInitialization section represents global settings !--- for the client. In some cases, for ! - --> <ClientInitialization> -- The Start Before Logon feature can be used to activate !--- the VPN as part of the logon sequence ·-> <UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon> - This control enables an administrator to have a one time !--- message displayed prior to a users

```
<ShowPreConnectMessage>false</ShowPreConnectMessage>
!-- This section enables the definition of various attributes !--- that can be used to refine client c
-->
<CertificateMatch>
!--- Certificate Distinguished Name matching allows !--- for exact match criteria in the choosing of a
 <DistinguishedName>
 <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
<Name>ISSUER-CN</Name>
<Pattern>DoD-Issuer-ABC</Pattern>
</DistinguishedNameDefinition>
</DistinguishedName>
</CertificateMatch>
</ClientInitialization>
!-- This section contains the list of hosts from which !--- the user is able to select.
<ServerList>
!--- This is the data needed to attempt a connection to !--- a specific host.
-->
<HostEntry>
<HostName>host-02</HostName>
<HostAddress>host-02.dod.gov</HostAddress>
</HostEntry>
 <HostEntry>
<HostName>host-01</HostName>
<HostAddress>192.168.1.1</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

相关信息

- X.509 和 RFC 3280 指定的证书和 CRL
- <u>RFC 2560 指定的 OCSP</u>
- Public Key Infrastructure 简介
- <u>草案标准分析的"轻量 OCSP"</u>
- RFC 2246 指定的 SSL/TLS

• <u>技术支持和文档 - Cisco Systems</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。