在 Cisco VPN 3000 集中器上通过 HTTP 检查 CRL

目录

简介

本文档介绍如何使用HTTP模式启用证书撤销列表(CRL)检查，以检查Cisco VPN 3000集中器中安装的证书颁发机构(CA)证书。

证书的整个有效期通常应该有效。但是，如果证书因名称更改、主题与CA之间的关联更改和安全危害等原因变为无效，CA将撤销证书。在X.509中，CA通过定期发出签名的CRL来撤销证书，其中每个已撤销的证书都由其序列号标识。启用CRL检查意味着每次VPN集中器使用证书进行身份验证时，它也会检查CRL，以确保所验证的证书未被撤销。

CA使用轻量级目录访问协议(LDAP)/HTTP数据库来存储和分发CRL。它们也可能使用其他方法，但VPN集中器依赖于LDAP/HTTP访问。

VPN集中器3.6版或更高版本中引入了HTTP CRL检查。但是，基于LDAP的CRL检查在早期的3.x版本中引入。本文档仅讨论使用HTTP进行CRL检查。

注意：VPN 3000系列集中器的CRL缓存大小取决于平台，无法根据管理员的愿望进行配置。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 您已使用用于互联网密钥交换(IKE)身份验证的证书成功从VPN 3.x硬件客户端建立IPsec隧道（未启用CRL检查）。
- 您的VPN集中器始终可以连接到CA服务器。
- 如果CA服务器连接到公共接口，则已在公共（默认）过滤器中打开必要的规则。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- VPN 3000集中器4.0.1 C版
- VPN 3.x硬件客户端
- 用于在Windows 2000服务器上运行的证书生成和CRL检查的Microsoft CA服务器。

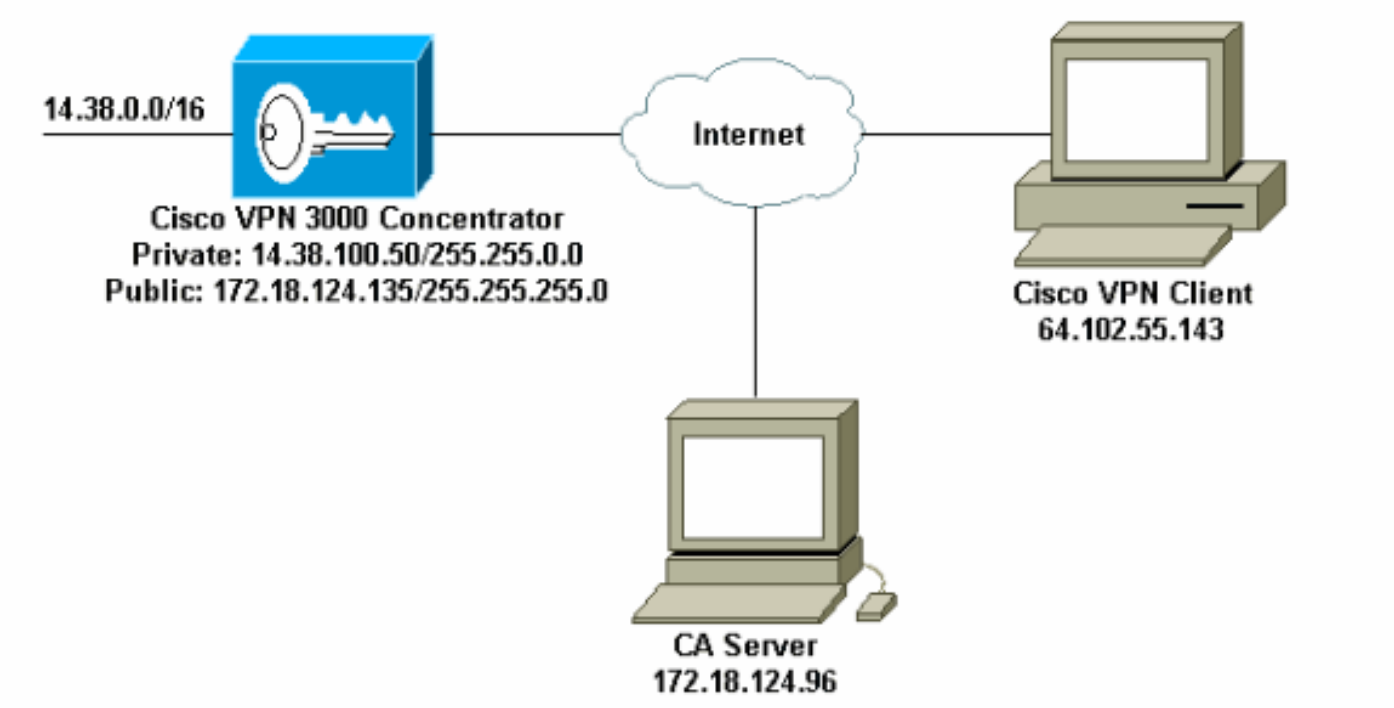
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

网络图

本文档使用以下网络设置：

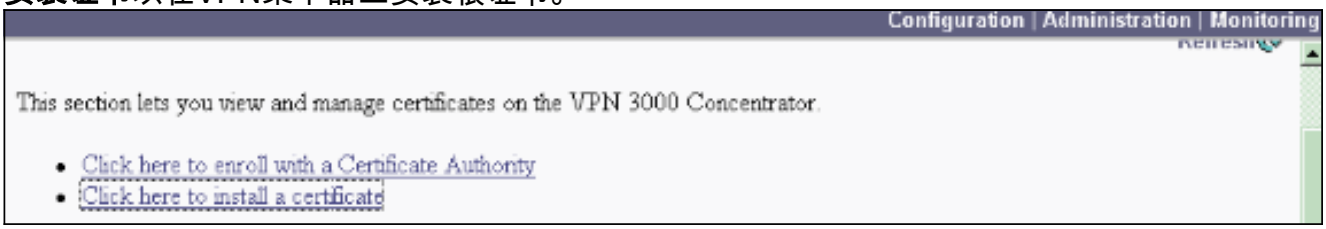


配置VPN 3000集中器

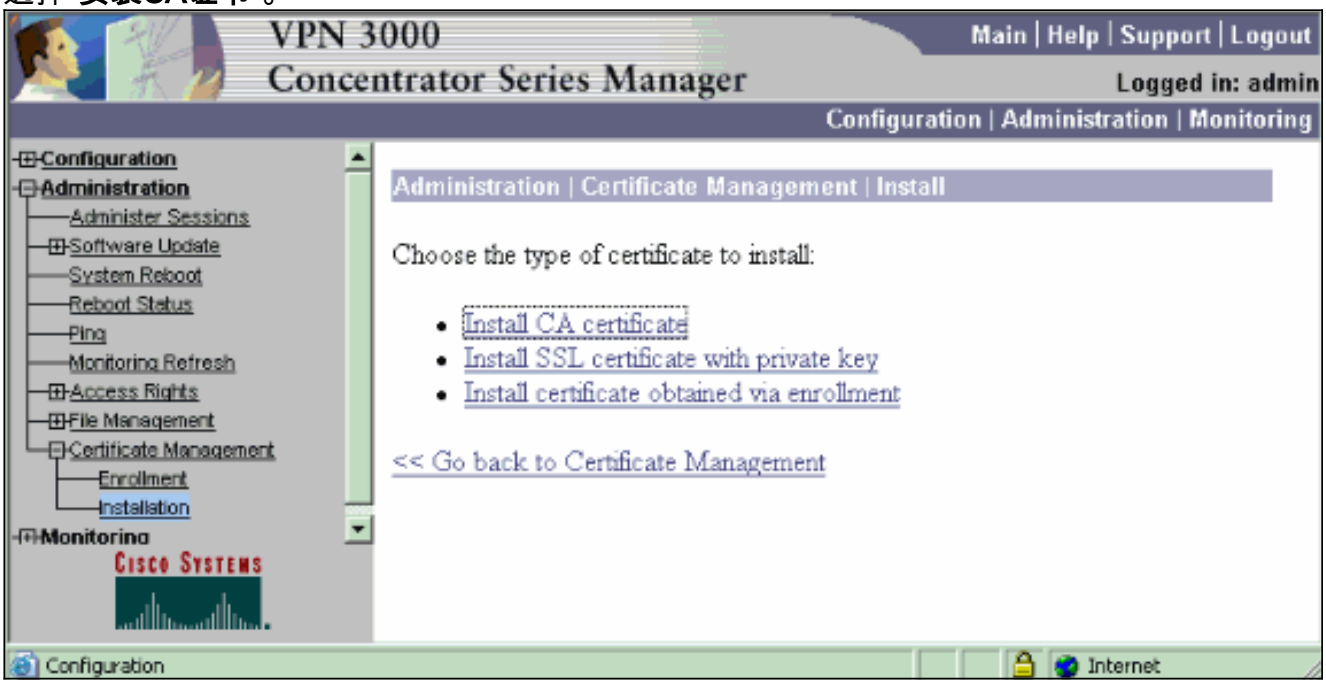
逐步指导

完成以下步骤以配置 VPN 3000 集中器：

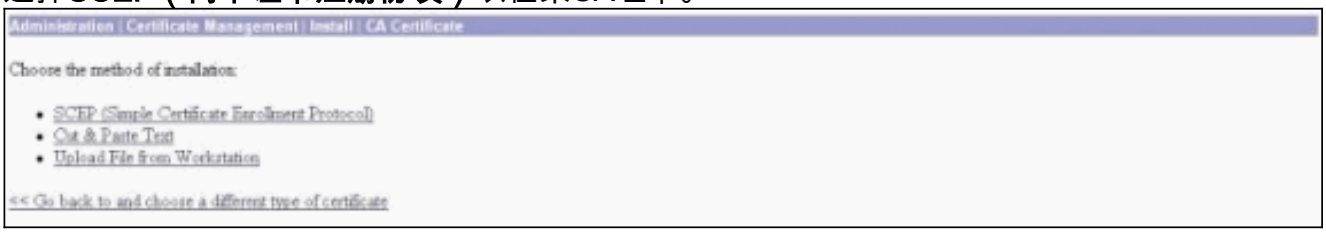
1. 如果您没有证书，请**选择Administration > Certificate Management** 请求证书。选择**单击此处安装证书**以在VPN集中器上安装根证书。



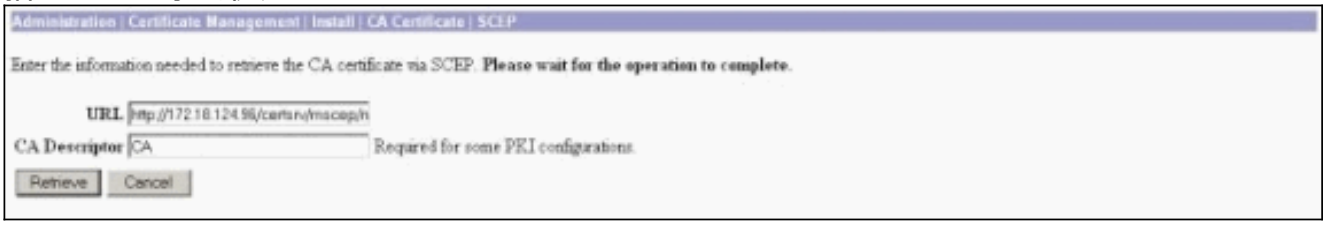
2. 选择“**安装CA证书**”。



3. 选择**SCEP（简单证书注册协议）**以检索CA证书。

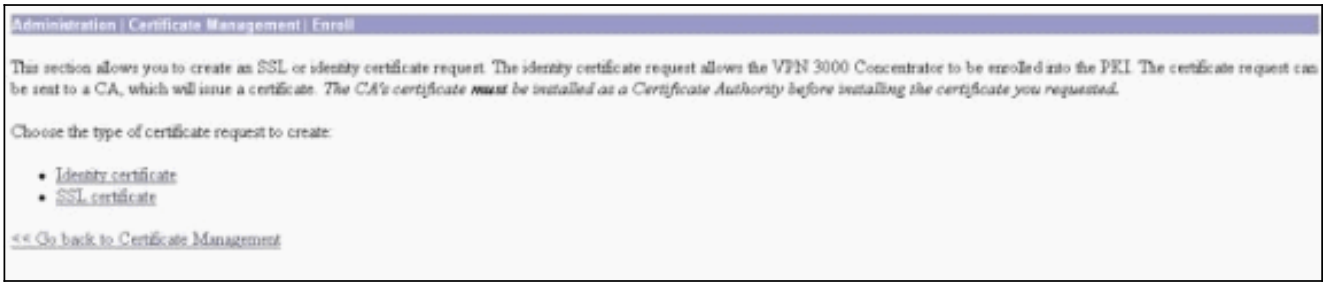


4. 在SCEP窗口中，在URL对话框中输入CA服务器的完整URL。在本例中，CA服务器的IP地址为172.18.124.96。由于此示例使用Microsoft的CA服务器，因此完整的URL为http://172.18.124.96/certsrv/mscep/mscep.dll。接下来，在CA描述符对话框中输入一个单词描述符。本示例使用CA。

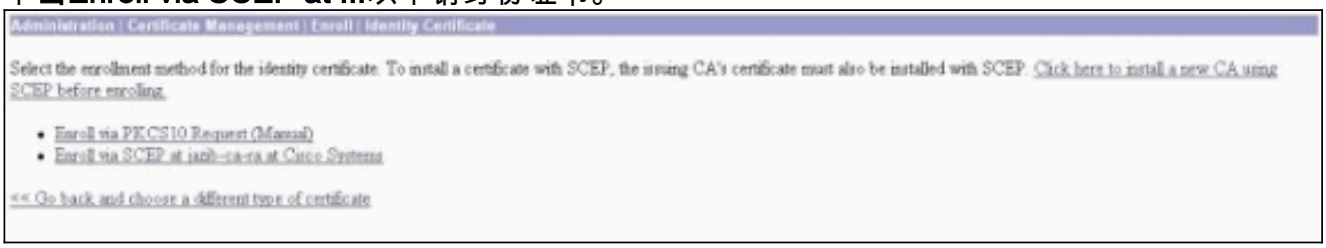


5. 单击 Retrieve（检索）。您的CA证书应显示在Administration > Certificate Management窗口下。如果您没有看到证书，请返回步骤1并再次执行该步骤。

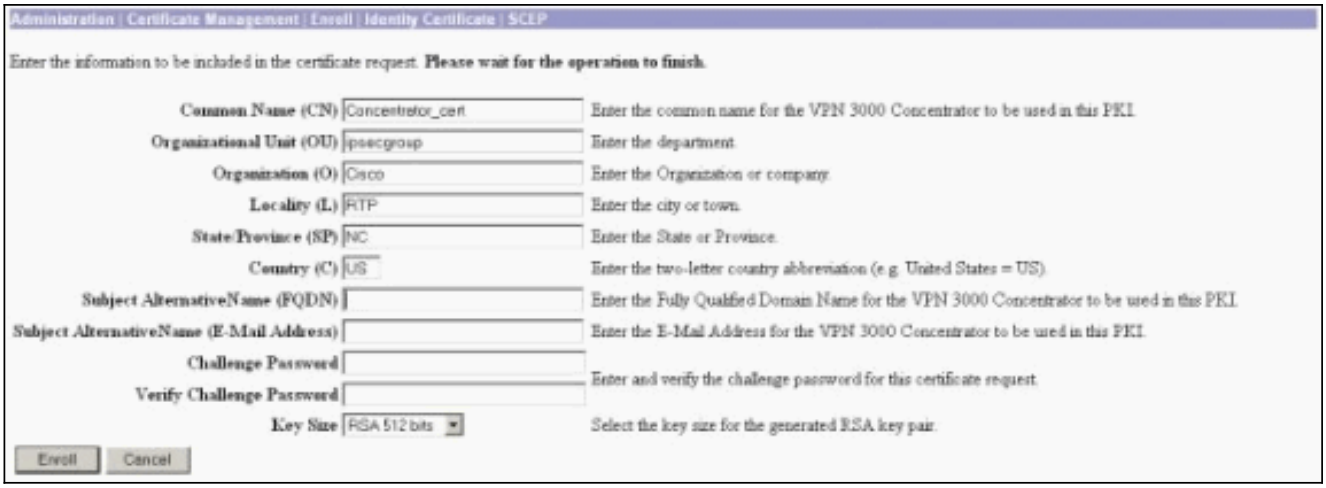
6. 获得CA证书后，选择**Administration > Certificate Management > Enroll**，然后单击**Identity certificate**。



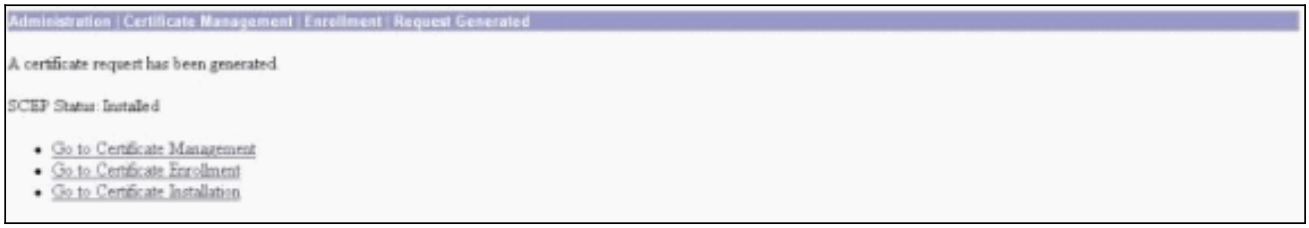
7. 单击**Enroll via SCEP at ...**以申请身份证书。



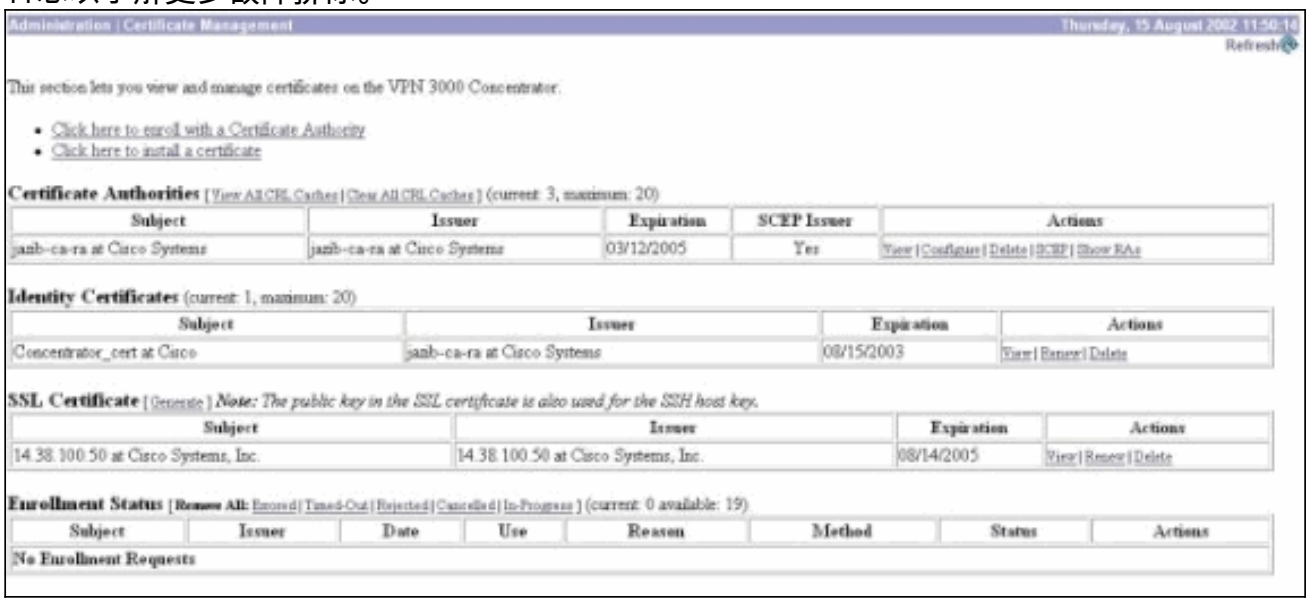
8. 完成以下步骤以填写登记表：在公用名(CN)字段中输入要在公用密钥基础设施(PKI)中使用的VPN集中器的公用名。在“组织单位(OU)”字段中输入您的部门。OU应与已配置的IPsec组名称匹配。在“组织(O)”字段中输入您的组织或公司。在Locality(L)字段中输入您的城市或城镇。在州/省(SP)字段中输入您所在的州或省。在国家/地区(C)字段中输入您的国家/地区。在完全限定域名(FQDN)字段中输入要在PKI中使用的VPN集中器的完全限定域名(FQDN)。在Subject Alternative Name(email Address)(主题备用名称（邮件地址）)字段中输入要在PKI中使用的VPN集中器的邮件地址。在质询密码字段中输入证书请求的质询密码。在Verify Challenge Password字段中重新输入质询密码。从Key Size下拉列表中选择生成的RSA密钥对的密钥大小。



9. 选择**Enroll**并查看轮询状态中的SCEP状态。
10. 转到CA服务器以批准身份证书。在CA服务器上获得批准后，您的SCEP状态应该为Installed。

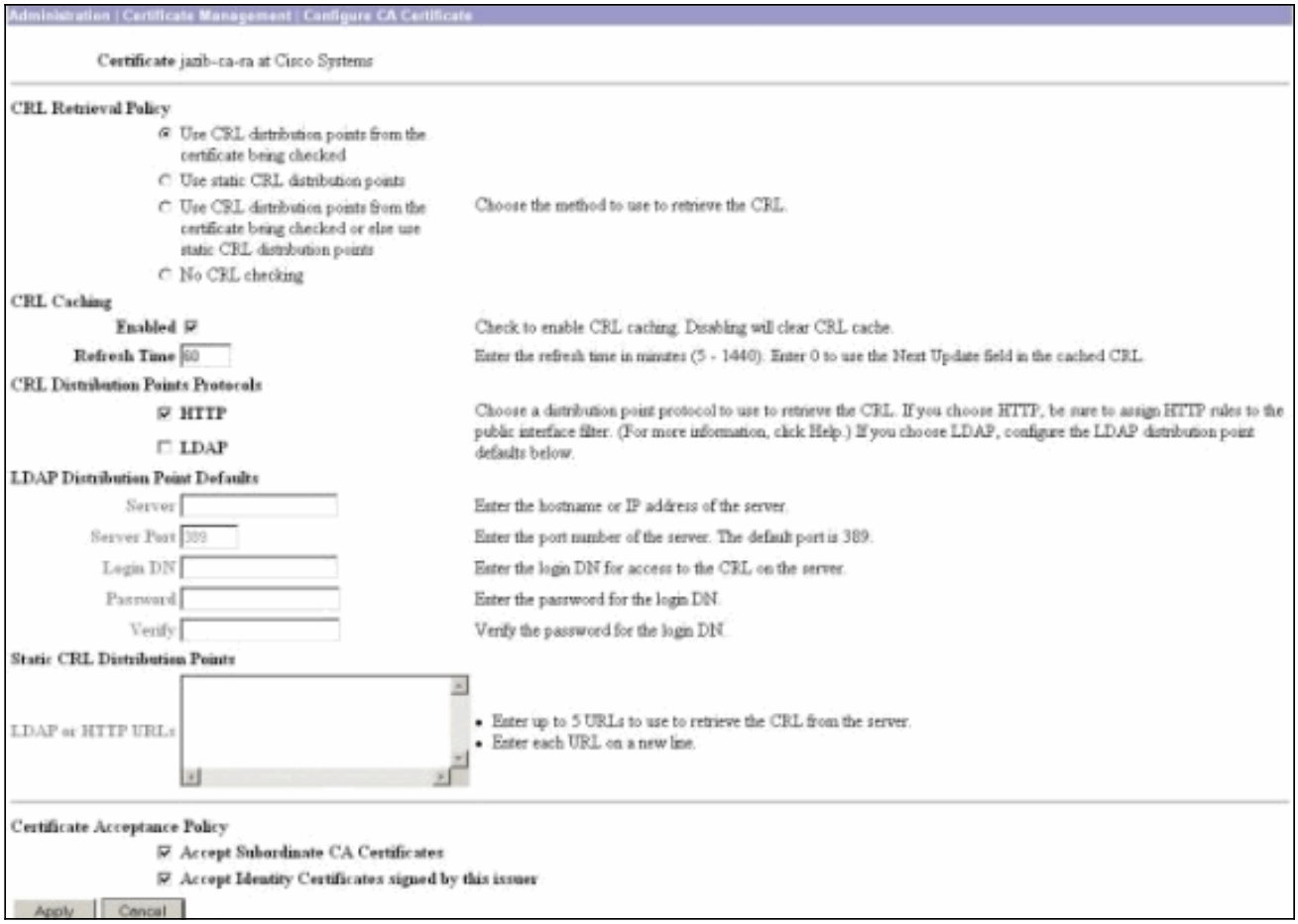


11. 在Certificate Management下，您应该看到您的身份证书。如果没有，请检查CA服务器上的日志以了解更多故障排除。



12. 选择**View**，查看您收到的证书是否具有CRL分发点(CDP)。CDP列出此证书颁发者的所有CRL分发点。如果证书上有CDP，并且使用DNS名称向CA服务器发送查询，请确保在VPN集中器中定义了DNS服务器，以使用IP地址解析主机名。在本例中，CA服务器的主机名称为jazib-pc，它解析为DNS服务器上的IP地址172.18.124.96。

13. 在CA证书上单击**Configure**，以对收到的证书启用CRL检查。如果您在收到的证书上具有CDP，并且您希望使用它，则从要检查的证书中选择**使用CRL分发点**。由于系统必须从网络分发点检索和检查CRL，因此启用CRL检查可能会缩短系统响应时间。此外，如果网络速度慢或拥塞，CRL检查可能会失败。启用CRL缓存以缓解这些潜在问题。这会将检索到的CRL存储在本地易失性内存中，因此允许VPN集中器更快地验证证书的撤销状态。启用CRL缓存后，VPN集中器首先检查缓存中是否存在所需的CRL，并在需要检查证书的撤销状态时根据CRL中的序列号列表检查证书的序列号。如果找到证书的序列号，则认为证书已撤销。VPN集中器从外部服务器检索CRL时，无论是在缓存中未找到所需的CRL时、缓存CRL的有效期已过时，还是在配置的刷新时间已过时。当VPN集中器从外部服务器接收新CRL时，它会使用新CRL更新缓存。缓存最多可包含64个CRL。**注意：**内存中存在CRL缓存。因此，重新启动VPN集中器会清除CRL缓存。VPN集中器在处理新的对等身份验证请求时，使用更新的CRL重新填充CRL缓存。如果选择**使用静态CRL分发点**，则可以使用最多五个静态CRL分发点，如此窗口中指定。如果选择此选项，必须至少输入一个URL。您也可以从正被检**查的证书中选择使用CRL分发点，或**选择使用**静态CRL分发点**。如果VPN集中器在证书中找不到五个CRL分发点，它会添加静态CRL分发点，最多限制为五个。如果选择此选项，请至少启用一个CRL分发点协议。您还必须至少输入一个（且不超过五个）静态CRL分发点。如果要**禁用CRL检**查，请选择No CRL Checking。在CRL Caching下，选择**Enabled**框，以允许VPN集中器缓存检索的CRL。默认不是启用CRL缓存。禁用CRL缓存（取消选中此框）时，CRL缓存将被清除。如果配置了使用CRL分发点的CRL检索策略，请选择要用于检索CRL的分发点协议。在本例中选择**HTTP**以检索CRL。如果CA服务器指向公共接口，则将HTTP规则分配给公共接口过滤器。



监控

选择**Administration > Certificate Management**，然后单击**View All CRL cache**，查看您的VPN集中器是否已缓存来自CA服务器的任何CRL。

验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

集中器中的日志

在VPN集中器上启用这些事件，以确保CRL检查工作正常。

1. 选择**Configuration > System > Events > Classes**以设置日志记录级别。
2. 在Class Name下，选择IKE、**IKEDBG**、IPSEC 、IPSECDBG或**CERT**。
3. 单击**Add**或**Modify**，然后选**择Severity to Log选项1-13**。
4. 如果要**修改**，请单击“应用”，如果**要添**加新条目，请单击“添加”。

成功的集中器日志

如果CRL检查成功，这些消息将在可过滤的事件日志中显示。

```
1315 08/15/2002 13:11:23.520 SEV=7 CERT/117 RPT=1
The requested CRL was found in cache.
The CRL Distribution point is: http://jazib-pc/CertEnroll/jazib-ca-ra.crl
```

```
1317 08/15/2002 13:11:23.520 SEV=8 CERT/46 RPT=1
CERT_CheckCrl(62f56e8, 0, 0)

1318 08/15/2002 13:11:23.520 SEV=7 CERT/2 RPT=1
Certificate has not been revoked: session = 2

1319 08/15/2002 13:11:23.530 SEV=8 CERT/50 RPT=1
CERT_Callback(62f56e8, 0, 0)

1320 08/15/2002 13:11:23.530 SEV=5 IKE/79 RPT=2 64.102.60.53
Group [ipsecgroup]
Validation of certificate successful
(CN=client_cert, SN=61521511000000000086)
```

有关成功集中器日志的完整输出，请参阅成功集中器日志。

失败日志

如果CRL签入不成功，这些消息将在可过滤的事件日志中显示。

```
1332 08/15/2002 18:00:36.730 SEV=7 CERT/6 RPT=2
Failed to retrieve revocation list: session = 5

1333 08/15/2002 18:00:36.730 SEV=7 CERT/114 RPT=2
CRL retrieval over HTTP has failed. Please make sure that proper filter rules
have been configured.

1335 08/15/2002 18:00:36.730 SEV=7 CERT/8 RPT=2
Error processing revocation list: session = 5, reason = Failed to retrieve CRL
from the server.
```

有关失败集中器日志的完整输出，请参阅已撤销集中器日志。

有关成功的客户端日志的完整输出，请参阅“成功的客户端日志”。

有关失败客户端日志的完整输出，请参阅已撤销客户端日志。

故障排除

有关故障排除的详细信息，请参阅VPN 3000集中器上的连接问题故障排除。

相关信息

- Cisco VPN 3000 系列集中器支持页面
- Cisco VPN 3000 Client 支持页
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems