

使用数字证书在 Windows 2000 和 VPN 3000 集中器之间进行的 L2TP Over IPsec 配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[目标](#)

[规则](#)

[获取根证明](#)

[获取客户端的一身份证书](#)

[使用网络连接向导，创建对VPN3000的一连接](#)

[配置VPN 3000集中器](#)

[获取根证明](#)

[获取VPN 3000集中器的一身份证书](#)

[配置客户端的一个池](#)

[配置IKE建议](#)

[配置SA](#)

[配置组和用户](#)

[调试信息](#)

[排除故障信息](#)

[相关信息](#)

简介

本文显示使用的逐步程序连接到从使用L2TP/IPsec嵌入客户端的Windows 2000客户端的VPN 3000集中器。假设，您使用数字证书(独立ROOT认证中心(CA)没有验证注册协议(CEP))验证您的对VPN集中器的连接。本文使用微软Certificate Service为说明。参考文档的 [Microsoft网站](#)关于怎样配置它。

注意： 只有因为Windows 2000屏幕的外观能更改，这是示例。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息是为Cisco VPN 3000集中器系列。

目标

在此步骤，您完成这些步骤：

1. 获取根证明。
2. 获取客户端的一身份证书。
3. 在网络连接向导帮助下创建对VPN3000的一连接。
4. 配置VPN 3000集中器。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

获取根证明

完成这些说明为了获取根证明：

1. 打开浏览器窗口并且输入微软认证授权的(通常http://servername或IP地址URL CA/certsrv)。证书检索和请求显示的Welcome窗口。
2. 在Welcome窗口下请选择任务，选择**获取CA证书或证书撤销列表**并且其次单击。
3. 从获取CA证书或证书撤销列表窗口，在左边角落点击**安装此CA证书路径**。这添加CA证书到可信的根证书权限存储。这意味着此所有的证书对此客户端的CA问题是委托。

获取客户端的身份证书

完成这些步骤为了获取客户端的一身份证书：

1. 打开浏览器窗口并且输入微软认证授权的URL (通常CA/certsrv的http://servername或IP地址)。证书检索和请求显示的Welcome窗口。
2. 从Welcome窗口，下请选择任务，选择**请求证书**，并且其次单击。
3. 从Choose Request Type窗口，请选择**Advanced请求**并且其次单击。
4. **使用表**，从先进的证书请求窗口，请选择**提交证书请求对此CA**。
5. 填写字段正如在此示例。部门(组织单位)需要的值能匹配在VPN集中器配置的组。请勿指定的密钥大小大于1024。请务必选择**使用本地机器存储**的复选框。当你完成的时候，**其次请单击**。基于关于怎样CA服务器配置，此窗口有时出现。如果它，与CA管理员联系。
6. 点击**霍姆**有上一步主屏幕，选择在**待定证书的检查**，并且其次单击。
7. 在证书发出的窗口，点击**安装此证书**。
8. 为了查看您的客户端证书，选择**Start > Run**，并且执行微软管理控制台(MMC)。
9. 点击**控制台**并且选择**添加/删除管理单元**。
10. 单击从列表**添加**并且选择**证书**。
11. 当请求您证书的范围的窗口出现时，请选择**计算机帐户**。
12. 验证CA服务器的证书查找在可靠的根证书颁发机构下。并且请验证您有一证书通过选择**控制台根>证书(本地计算机)>个人>证书**，如此镜像所显示。

[使用网络连接向导，创建对VPN3000的连接](#)

完成此步骤为了在网络连接向导帮助下创建对VPN3000的一连接：

1. 用鼠标右键单击**我的网络空间**，选择**属性**并且点击**Make New Connection**。
2. 从Network Connection Type窗口，请选择**连接对私有网络通过互联网**其次然后单击。
3. 输入VPN集中器的公共接口的主机名或IP地址，并且**其次**单击。
4. 在连接可用性窗口，为**我自己**请仅选择并且**其次**单击。
5. 在公共网络窗口，是否请选择自动地拨号初始连接(ISP帐户)。
6. 在Destination Address屏幕，请输入VPN 3000集中器的主机名或IP地址，并且**其次**单击。
7. 在Network Connection Wizard窗口，请输入一名称对于连接并且点击**芬通社**。在本例中，连接被命名“思科公司VPN”。
8. 在Virtual Private Connection窗口，点击**属性**。
9. 在属性窗口上，选择Networking选项。
10. 在Type of VPN server I am calling下，请从下拉菜单选择**L2TP**，突出显示**互联网协议TCP/IP**，并且点击**属性**。
11. 选择**Advanced > Options > Properties**。
12. 在IP安全窗口，请选择**使用此IP安全策略**。
13. 从下拉菜单选择**客户端(只请响应)**策略，并且点击OK键几次，直到您回到Connect屏幕。
14. 为了首次连接，输入您的用户名和密码，和点击**连接**。

[配置VPN 3000集中器](#)

[获取根证明](#)

完成这些步骤为了获取VPN 3000集中器的一个根证明：

1. 点您的浏览器您的CA (通常某事例如http://ip_add_of_ca/certsrv/)，**获取CA证书或证书撤销列表**，并且**其次**单击。
2. 点击**下载CA证书**并且保存文件某处在您的本地磁盘。
3. 在VPN 3000集中器上，请选择**Administration > Certificate Management**，并且单击**点击此处安装证书和安装CA证书**。
4. 点击**从工作站的上传文件**。
5. 单击**浏览**并且选择您下载的CA证书文件。
6. 突出显示文件名并且点击**安装**。

[获取VPN 3000集中器的身份证书](#)

完成这些步骤为了获取VPN 3000集中器的一身份证书：

1. 选择**ConfAdministration > Certificate Management > 登记>身份证书**，然后单击**通过PKCS10 Request(Manual)登记**。填好表格如显示此处并且单击**登记**。浏览器窗口冒出与证书请求。它需要包含文本类似于此输出：-----BEGIN NEW CERTIFICATE REQUEST-----

```
MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMDAwLW5hbWUxDDAKBgNVBAsTA3Nu
czEOMAwGA1UEChMFY21zY28xDDAKBgNVBACjTA2J4bDELMakGA1UEBhMCYmUwWjAN
BgkqhkiG9w0BAQEFAANJADBGAkEAX7K+pve004qILNNw3kPVWXrdlqZV4yeOIPdh
C8/V5Yuuq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG
SIb3DQEJdjElMCMwIQYDVORBBowGIIWdnBuMzAwMCluYW11LmNpc2NvLmNvbTAN
```

BgkqhkIG9w0BAQQFAANBABzcG3IKaWnDLFtrNf1QDi+D7w8dxPu74b/BRHn9fsKI
X6+X0ed0EuEgm1/2nfj8Ux0nV5F/c5wukUfysMmJ/ak=
-----END NEW CERTIFICATE REQUEST-----

2. 点您的浏览器您的CA服务器，检查请求证书，并且其次单击。
3. 使用a base64 encoded PKCS -7 file，检查高级请求，其次单击，并且选择提交证书请求使用a base64 encoded PKCS -10 file或续订请求。
4. 单击 Next。剪贴在正文以前显示的证书请求的文本。单击 submit。
5. 基于关于怎样CA服务器配置，您能点击下载CA证书。或者，因为证书由CA很快发出，去上一步您的CA服务器并且检查在一待定证书的检查。
6. 点击下，选择您的请求，并且其次再单击。
7. 点击下载CA证书，并且保存在本地磁盘的文件。
8. 在VPN 3000集中器上，请选择Administration > Certificate Management > Install，并且点击通过登记获取的安装证书。您然后看到您的挂起请求以状态“进展中”，正如在此镜像。
9. 点击安装，跟随由从工作站的上传文件。
10. 单击浏览并且选择包含CA发出的您的证书的文件。
11. 突出显示文件名并且点击安装。
12. 选择 Administration > Certificate Management。屏幕类似于此镜像出现。

配置客户端的池

完成此步骤为了配置客户端的一个池：

1. 为了分配一可用的IP地址范围，请点一个浏览器VPN 3000集中器的内部接口并且选择 Configuration > System > Address Management > Pools > Add。
2. 指定IP地址范围与在网络内部的任何其它设备不相冲突，并且单击添加。
3. 为了告诉VPN 3000集中器使用池，选择Configuration > System > Address Management > Assignment，检查使用地址池方框，和在此镜像单击应用，正如。

配置IKE建议

完成这些步骤为了配置IKE建议：

1. 如此镜像所显示，选择Configuration > System > Tunneling Protocols > IPSec > IKE Proposals，单击添加并且选择参数。
2. 单击添加，突出显示在正确列的新的建议，并且单击激活。

配置SA

完成此步骤为了配置安全关联(SA)：

1. 选择Configuration > Policy Management > Traffic Management > SA并且点击ESP-L2TP-TRANSPORT。如果此SA不是可用的或，如果使用它若干其他目的，请创建新的SA类似于这一个。SA的不同的设置是可接受。更改根据您的安全策略的此参数。
2. 选择您以前配置在数字证书下拉菜单下的数字证书。选择win2000的IKE Internet Key Exchange (IKE)建议。注意：这不是必须。当L2TP/IPsec客户端连接到VPN集中器时，所有IKE建议配置在页Configuration > System > Tunneling Protocols > IPSec > IKE Proposals的活动列下按顺序尝试。此镜像显示为SA需要的配置：

配置组 and 用户

完成此步骤为了配置组 and 用户：

1. 选择 **Configuration > User Management > Base Group**。
2. 在常规选项卡下，请确保IPSec上的L2TP被检查。
3. 在IPSec选项下，请选择**ESP-L2TP-TRANSPORT SA**。
4. 在PPTP/L2TP选项卡下，请不选定所有L2TP加密选项。
5. 选择 **Configuration > User Management > Users** 并且单击**添加**。
6. 输入您使用从您的Windows 2000客户端连接的名称和密码。确保您选择**基本组**在组选择下。
7. 在常规选项卡下，请检查IPSec上的L2TP隧道协议。
8. 在IPSec选项下，请选择**ESP-L2TP-TRANSPORT SA**。
9. 在PPTP/L2TP选项卡下，请不选定所有L2TP加密选项，并且单击**添加**。您当前能在L2TP/IPsec Windows 2000客户端帮助下连接。**注意：**您选择配置基本组接受远程L2TP/IPsec连接。配置匹配SA组织单位(OU)字段接受流入连接的组也是可能的。配置是相同的。

调试信息

```
269 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3868 10.48.66.76
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 7

271 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3869 10.48.66.76
Phase 1 failure against global IKE proposal # 16:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

274 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3870 10.48.66.76
Proposal # 1, Transform # 2, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

279 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3871 10.48.66.76
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

282 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3872 10.48.66.76
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

285 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3873 10.48.66.76
Phase 1 failure against global IKE proposal # 4:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

288 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3874 10.48.66.76
```

Phase 1 failure against global IKE proposal # 5:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

291 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3875 10.48.66.76
Phase 1 failure against global IKE proposal # 6:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

294 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3876 10.48.66.76
Phase 1 failure against global IKE proposal # 7:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

297 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3877 10.48.66.76
Phase 1 failure against global IKE proposal # 8:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

300 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3878 10.48.66.76
Phase 1 failure against global IKE proposal # 9:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

303 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3879 10.48.66.76
Phase 1 failure against global IKE proposal # 10:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

306 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3880 10.48.66.76
Phase 1 failure against global IKE proposal # 11:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

309 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3881 10.48.66.76
Phase 1 failure against global IKE proposal # 12:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

312 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3882 10.48.66.76
Phase 1 failure against global IKE proposal # 13:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

315 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3883 10.48.66.76
Phase 1 failure against global IKE proposal # 14:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

318 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3884 10.48.66.76
Phase 1 failure against global IKE proposal # 15:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 7

321 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3885 10.48.66.76
Phase 1 failure against global IKE proposal # 16:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

324 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3886 10.48.66.76
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

329 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3887 10.48.66.76
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

332 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3888 10.48.66.76
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

335 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3889 10.48.66.76
Phase 1 failure against global IKE proposal # 4:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

338 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3890 10.48.66.76
Phase 1 failure against global IKE proposal # 5:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

341 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3891 10.48.66.76
Phase 1 failure against global IKE proposal # 6:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

344 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3892 10.48.66.76
Phase 1 failure against global IKE proposal # 7:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

347 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3893 10.48.66.76
Phase 1 failure against global IKE proposal # 8:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

350 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3894 10.48.66.76
Phase 1 failure against global IKE proposal # 9:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

353 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3895 10.48.66.76

Phase 1 failure against global IKE proposal # 10:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

356 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3896 10.48.66.76
Phase 1 failure against global IKE proposal # 11:
Mismatched attr types for class Hash Alg:
Rcv'd: SHA
Cfg'd: MD5

358 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3897 10.48.66.76
Phase 1 failure against global IKE proposal # 12:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

361 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3898 10.48.66.76
Phase 1 failure against global IKE proposal # 13:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

364 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3899 10.48.66.76
Phase 1 failure against global IKE proposal # 14:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

367 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3900 10.48.66.76
Phase 1 failure against global IKE proposal # 15:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 7

370 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3901 10.48.66.76
Phase 1 failure against global IKE proposal # 16:
Mismatched attr types for class Hash Alg:
Rcv'd: SHA
Cfg'd: MD5

372 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3902 10.48.66.76
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

377 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3903 10.48.66.76
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

380 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3904 10.48.66.76
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

383 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3905 10.48.66.76
Phase 1 failure against global IKE proposal # 4:
Mismatched attr types for class Encryption Alg:

Rcv'd: DES-CBC
Cfg'd: Triple-DES

386 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3906 10.48.66.76
Phase 1 failure against global IKE proposal # 5:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

389 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3907 10.48.66.76
Phase 1 failure against global IKE proposal # 6:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

392 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3908 10.48.66.76
Phase 1 failure against global IKE proposal # 7:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

395 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3909 10.48.66.76
Phase 1 failure against global IKE proposal # 8:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

398 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3910 10.48.66.76
Phase 1 failure against global IKE proposal # 9:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

401 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3911 10.48.66.76
Phase 1 failure against global IKE proposal # 10:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

404 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3912 10.48.66.76
Phase 1 failure against global IKE proposal # 11:
Mismatched attr types for class Auth Method:
Rcv'd: RSA signature with Certificates
Cfg'd: Preshared Key

407 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3913 10.48.66.76
Phase 1 failure against global IKE proposal # 12:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

410 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3914 10.48.66.76
Phase 1 failure against global IKE proposal # 13:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

413 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3915 10.48.66.76
Phase 1 failure against global IKE proposal # 14:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

416 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3916 10.48.66.76

Phase 1 failure against global IKE proposal # 15:

Mismatched attr types for class DH Group:

Rcv'd: Oakley Group 1

Cfg'd: Oakley Group 7

419 02/15/2002 12:47:24.430 SEV=7 IKEDBG/28 RPT=20 10.48.66.76
IKE SA Proposal # 1, Transform # 4 acceptable
Matches global IKE entry # 16

420 02/15/2002 12:47:24.440 SEV=9 IKEDBG/0 RPT=3917 10.48.66.76
constructing ISA_SA for isakmp

421 02/15/2002 12:47:24.490 SEV=8 IKEDBG/0 RPT=3918 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 80

423 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3919 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

425 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3920 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

427 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3921 10.48.66.76
processing ke payload

428 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3922 10.48.66.76
processing ISA_KE

429 02/15/2002 12:47:24.540 SEV=9 IKEDBG/1 RPT=104 10.48.66.76
processing nonce payload

430 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3923 10.48.66.76
constructing ke payload

431 02/15/2002 12:47:24.600 SEV=9 IKEDBG/1 RPT=105 10.48.66.76
constructing nonce payload

432 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3924 10.48.66.76
constructing certreq payload

433 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3925 10.48.66.76
Using initiator's certreq payload data

434 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=61 10.48.66.76
constructing Cisco Unity VID payload

435 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=62 10.48.66.76
constructing xauth V6 VID payload

436 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=39 10.48.66.76
Send IOS VID

437 02/15/2002 12:47:24.600 SEV=9 IKEDBG/38 RPT=20 10.48.66.76
Constructing VPN 3000 spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)

439 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=63 10.48.66.76
constructing VID payload

440 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=40 10.48.66.76
Send Altiga GW VID

441 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3926 10.48.66.76
Generating keys for Responder...

442 02/15/2002 12:47:24.610 SEV=8 IKEDBG/0 RPT=3927 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 229

445 02/15/2002 12:47:24.640 SEV=8 IKEDBG/0 RPT=3928 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + CERT_REQ (7) + NONE (0)
... total length : 1186

448 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=106 10.48.66.76
Processing ID

449 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3929 10.48.66.76
processing cert payload

450 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=107 10.48.66.76
processing RSA signature

451 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3930 10.48.66.76
computing hash

452 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3931 10.48.66.76
processing cert request payload

453 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3932 10.48.66.76
Storing cert request payload for use in MM msg 4

454 02/15/2002 12:47:24.650 SEV=9 IKEDBG/23 RPT=20 10.48.66.76
Starting group lookup for peer 10.48.66.76

455 02/15/2002 12:47:24.650 SEV=9 IKE/21 RPT=12 10.48.66.76
No Group found by matching IP Address of Cert peer 10.48.66.76

456 02/15/2002 12:47:24.650 SEV=9 IKE/20 RPT=12 10.48.66.76
No Group found by matching OU(s) from ID payload:
ou=sns,

457 02/15/2002 12:47:24.650 SEV=9 IKE/0 RPT=12 10.48.66.76
Group [VPNC_Base_Group]
No Group name for IKE Cert session, defaulting to BASE GROUP

459 02/15/2002 12:47:24.750 SEV=7 IKEDBG/0 RPT=3933 10.48.66.76
Group [VPNC_Base_Group]
Found Phase 1 Group (VPNC_Base_Group)

460 02/15/2002 12:47:24.750 SEV=7 IKEDBG/14 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
Authentication configured for Internal

461 02/15/2002 12:47:24.750 SEV=9 IKEDBG/19 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
IKEGetUserAttributes: default domain = fenetwork.com

462 02/15/2002 12:47:24.770 SEV=5 IKE/79 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Validation of certificate successful
(CN=my_name, SN=6102861F000000000005)

464 02/15/2002 12:47:24.770 SEV=7 IKEDBG/0 RPT=3934 10.48.66.76
Group [VPNC_Base_Group]

peer ID type 9 received (DER_ASN1_DN)

465 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=108 10.48.66.76
Group [VPNC_Base_Group]
constructing ID

466 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3935 10.48.66.76
Group [VPNC_Base_Group]
constructing cert payload

467 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=109 10.48.66.76
Group [VPNC_Base_Group]
constructing RSA signature

468 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3936 10.48.66.76
Group [VPNC_Base_Group]
computing hash

469 02/15/2002 12:47:24.800 SEV=9 IKEDBG/46 RPT=64 10.48.66.76
Group [VPNC_Base_Group]
constructing dpd vid payload

470 02/15/2002 12:47:24.800 SEV=8 IKEDBG/0 RPT=3937 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) + NONE (0)
... total length : 1112

473 02/15/2002 12:47:24.800 SEV=4 IKE/119 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 1 COMPLETED

474 02/15/2002 12:47:24.800 SEV=6 IKE/121 RPT=4 10.48.66.76
Keep-alive type for this connection: None

475 02/15/2002 12:47:24.800 SEV=6 IKE/122 RPT=4 10.48.66.76
Keep-alives configured on but peer does not support keep-alives (type = None)

476 02/15/2002 12:47:24.800 SEV=7 IKEDBG/0 RPT=3938 10.48.66.76
Group [VPNC_Base_Group]
Starting phase 1 rekey timer: 21600000 (ms)

477 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3939 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 1108

480 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3940 10.48.66.76
Group [VPNC_Base_Group]
processing hash

481 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3941 10.48.66.76
Group [VPNC_Base_Group]
processing SA payload

482 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=110 10.48.66.76
Group [VPNC_Base_Group]
processing nonce payload

483 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=111 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

484 02/15/2002 12:47:24.810 SEV=5 IKE/25 RPT=4 10.48.66.76
Group [VPNC_Base_Group]

Received remote Proxy Host data in ID Payload:
Address 10.48.66.76, Protocol 17, Port 1701

487 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=112 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

488 02/15/2002 12:47:24.810 SEV=5 IKE/24 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received local Proxy Host data in ID Payload:
Address 10.48.66.109, Protocol 17, Port 0

491 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3942
QM IsRekeyed old sa not found by addr

492 02/15/2002 12:47:24.810 SEV=5 IKE/66 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IKE Remote Peer configured for SA: ESP-L2TP-TRANSPORT

493 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3943 10.48.66.76
Group [VPNC_Base_Group]
processing IPSEC SA

494 02/15/2002 12:47:24.810 SEV=7 IKEDBG/27 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IPSec SA Proposal # 1, Transform # 1 acceptable

495 02/15/2002 12:47:24.810 SEV=7 IKEDBG/0 RPT=3944 10.48.66.76
Group [VPNC_Base_Group]
IKE: requesting SPI!

496 02/15/2002 12:47:24.810 SEV=8 IKEDBG/6 RPT=4
IKE got SPI from key engine: SPI = 0x10d19e33

497 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3945 10.48.66.76
Group [VPNC_Base_Group]
oakley constructing quick mode

498 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3946 10.48.66.76
Group [VPNC_Base_Group]
constructing blank hash

499 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3947 10.48.66.76
Group [VPNC_Base_Group]
constructing ISA_SA for ipsec

500 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=113 10.48.66.76
Group [VPNC_Base_Group]
constructing ipsec nonce payload

501 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=114 10.48.66.76
Group [VPNC_Base_Group]
constructing proxy ID

502 02/15/2002 12:47:24.820 SEV=7 IKEDBG/0 RPT=3948 10.48.66.76
Group [VPNC_Base_Group]
Transmitting Proxy Id:
Remote host: 10.48.66.76 Protocol 17 Port 1701
Local host: 10.48.66.109 Protocol 17 Port 0

506 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3949 10.48.66.76
Group [VPNC_Base_Group]
constructing qm hash

```
507 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3950 10.48.66.76
SENDING Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

510 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3951 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

512 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3952 10.48.66.76
Group [VPNC_Base_Group]
processing hash

513 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3953 10.48.66.76
Group [VPNC_Base_Group]
loading all IPSEC SAs

514 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=115 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

515 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=116 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

516 02/15/2002 12:47:24.830 SEV=7 IKEDBG/0 RPT=3954 10.48.66.76
Group [VPNC_Base_Group]
Loading host:
  Dst: 10.48.66.109
  Src: 10.48.66.76

517 02/15/2002 12:47:24.830 SEV=4 IKE/49 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Security negotiation complete for User ()
Responder, Inbound SPI = 0x10d19e33, Outbound SPI = 0x15895ab9

520 02/15/2002 12:47:24.830 SEV=8 IKEDBG/7 RPT=4
IKE got a KEY_ADD msg for SA: SPI = 0x15895ab9

521 02/15/2002 12:47:24.830 SEV=8 IKEDBG/0 RPT=3955
pitcher: rcv KEY_UPDATE, spi 0x10d19e33

522 02/15/2002 12:47:24.830 SEV=4 IKE/120 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 2 COMPLETED (msgid=781ceadc)

523 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3956
pitcher: rcv KEY_SA_ACTIVE spi 0x10d19e33

524 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3957
KEY_SA_ACTIVE no old rekey centry found with new spi 0x10d19e33, mess_id 0x0
```

[排除故障信息](#)

此部分说明一些常见问题和故障排除方法中的每一的。

- 服务器不可能开始。很可能，IPSec服务没有开始。选择**Start > Programs > Administrative Tools > 服务**并且确保**IPSec服务**启用。
- **Error 786**：没有有效机器认证。此错误指示与证书的一问题在本地设备。为了容易地查看您的证书，请选择**Start > Run**，并且执行MMC。点击**控制台**并且选择**添加/删除管理单元**。单击从列表**添加**并且选择**证书**。当请求您证书的范围的窗口出现时，请选择**计算机帐户**。现在您能验

证CA服务器的证书查找在可靠的根证书颁发机构下。您能也验证您有一证书通过选择控制台根>证书(本地计算机)>个人>证书，如此镜像所显示。点击证书。验证一切正确。在本例中，有专用密钥关联与证书。然而，此证书超时。这是问题的原因。

- Error 792 : 安全协商超时。此消息在长时间之后出现。打开相关调试按照[Cisco VPN 3000集中器FAQ说明](#)。通过他们读。您需要发现事类似于此输出：9337 02/15/2002 15:06:13.500 SEV=8 IKEDBG/0 RPT=7002 10.48.66.76

```
Phase 1 failure against global IKE proposal # 6:
Mismatched attr types for class DH Group:
  Rcv'd: Oakley Group 1
  Cfg'd: Oakley Group 2
```

9340 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7003 10.48.66.76

```
Phase 1 failure against global IKE proposal # 7:
Mismatched attr types for class Auth Method:
  Rcv'd: RSA signature with Certificates
  Cfg'd: Preshared Key
```

9343 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7004 10.48.66.76

```
Phase 1 failure against global IKE proposal # 8:
Mismatched attr types for class DH Group:
  Rcv'd: Oakley Group 1
  Cfg'd: Oakley Group 7
```

9346 02/15/2002 15:06:13.510 SEV=7 IKEDBG/0 RPT=7005 10.48.66.76

All SA proposals found unacceptable

9347 02/15/2002 15:06:13.510 SEV=4 IKE/48 RPT=37 10.48.66.76

Error processing payload: Payload ID: 1

9348 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7006 10.48.66.76

```
IKE SA MM:261e40dd terminating:
flags 0x01000002, refcnt 0, tuncnt 0
```

9349 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7007

sending delete message 这表明IKE建议未适当地配置。验证从[配置](#)本文的[IKE建议](#)部分的信息。

- Error 789 : 安全层遇到处理错误。打开相关调试按照[Cisco VPN 3000集中器FAQ说明](#)。通过他们读。您需要发现事类似于此输出：11315 02/15/2002 15:36:32.030 SEV=8 IKEDBG/0 RPT=7686 Proposal # 1, Transform # 2, Type ESP, Id DES-CBC

```
Parsing received transform:
Phase 2 failure:
Mismatched attr types for class Encapsulation:
  Rcv'd: Transport
  Cfg'd: Tunnel
```

11320 02/15/2002 15:36:32.030 SEV=5 IKEDBG/0 RPT=7687

AH proposal not supported

11321 02/15/2002 15:36:32.030 SEV=4 IKE/0 RPT=27 10.48.66.76

```
Group [VPNC_Base_Group]
All IPSec SA proposals found unacceptable!
```

- 版本使用选择Monitoring > System Status查看此输出：VPN Concentrator Type: 3005
Bootcode Rev: Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 2000 05:36:41
Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Version 3.5.Rel Nov 27 2001 13:35:16
Up For: 44:39:48
Up Since: 02/13/2002 15:49:59
RAM Size: 32 MB

[相关信息](#)

- [IPSec协商/IKE协议产品支持](#)
- [技术支持 - Cisco Systems](#)