

# Habilitando o suporte à Certification Revocation List no VPN 3000 Series Concentrator

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Permita o suporte Idap no Certificate Authority](#)

[Peça o certificado de identidade no VPN 3000 concentrator](#)

[Peça o certificado de identidade no cliente VPN](#)

[Permita o apoio CRL no VPN 3000 concentrator](#)

[HTTP](#)

[LDAP](#)

[Entre o DN](#)

[Senha](#)

[LDAP ou URL do HTTP](#)

[Horas da atualização](#)

[Reforce a atualização seguinte](#)

[Debugs](#)

[VPN 3000 Concentrator](#)

[Cliente de VPN](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento descreve como permitir o Certification Revocation List (CRL) que verifica o apoio no VPN 3000 series concentrator.

## [Pré-requisitos](#)

### [Requisitos](#)

Não existem requisitos específicos para este documento.

### [Componentes Utilizados](#)

A informação neste documento aplica aos estes a versão de software e hardware:

- Versão de software 4.1.x do Cisco VPN 3000 Concentrator
- Versão Cliente VPN Cisco 4.x
- Microsoft certificate server

**Nota:** O Microsoft certificate server é usado neste exemplo. Contudo, a instalação dos Certificados com o uso de outros server do Certification Authority (CA) é similar. Os server apoiados de CA são alistados no [cliente VPN para Windows, liberam o 3.0](#).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

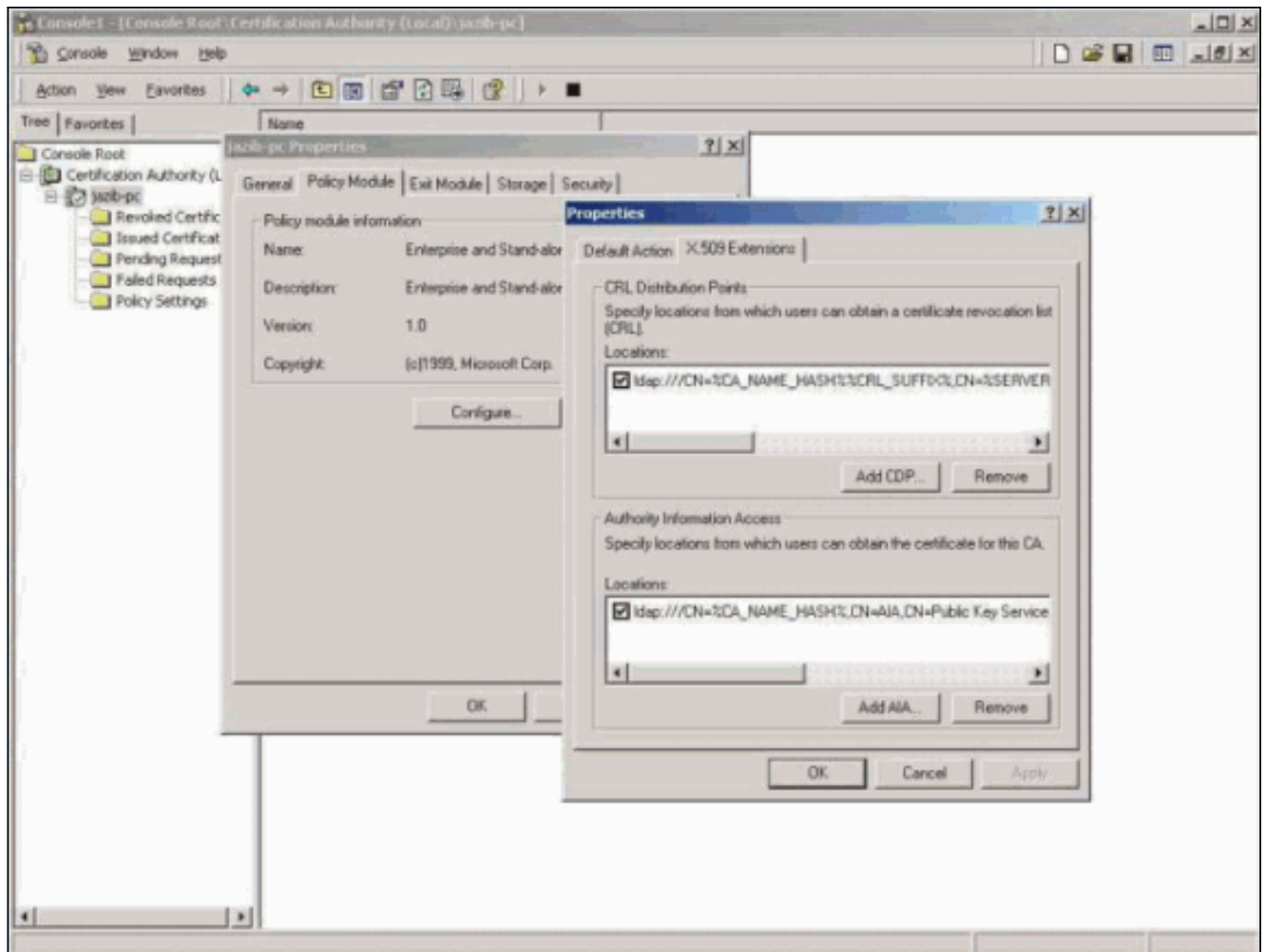
## Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

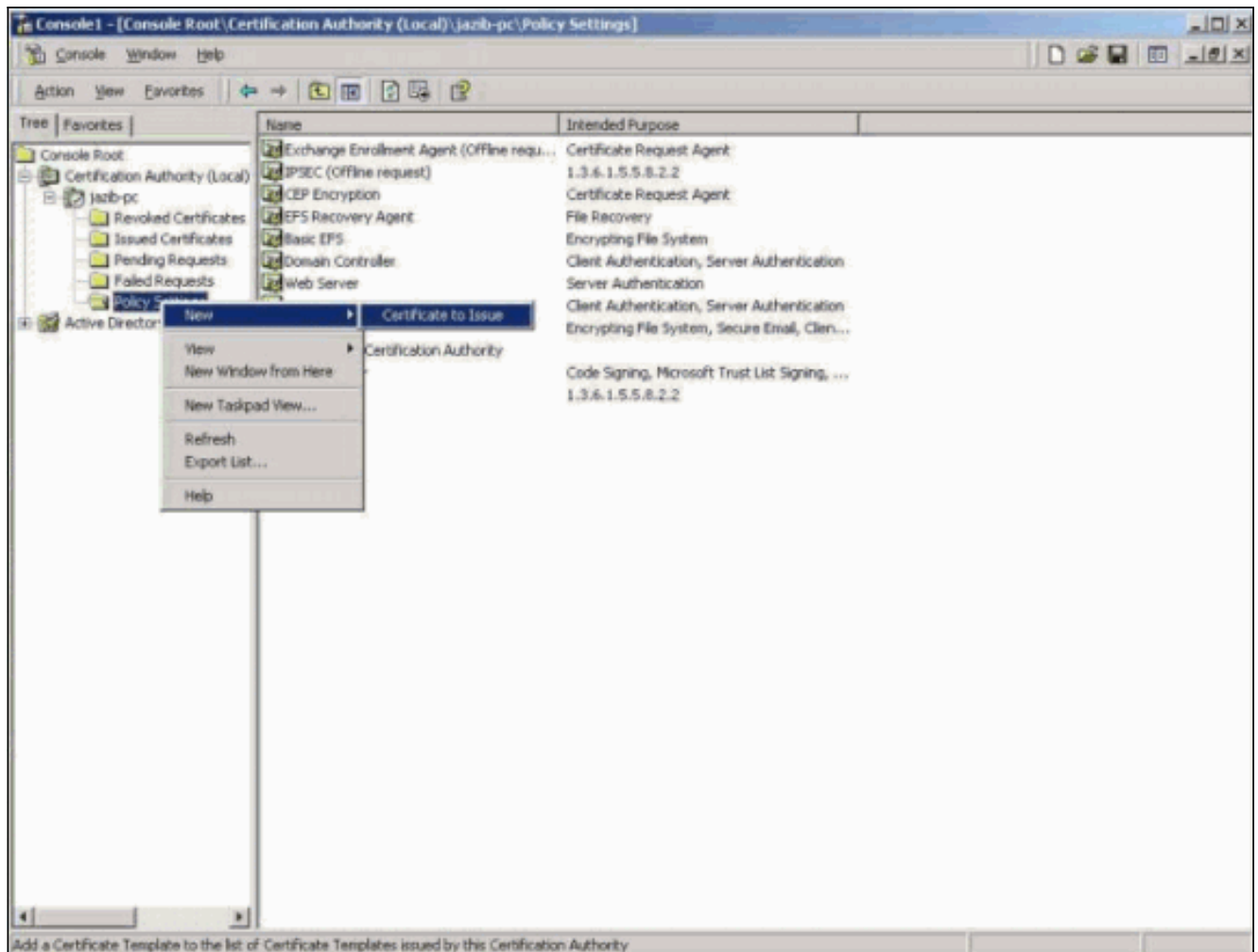
## Permita o suporte ldap no Certificate Authority

O VPN 3000 concentrator apoia somente o Lightweight Directory Access Protocol (LDAP) - verificação CRL baseada. Se você usa o server de CA de Microsoft, certifique-se de que você executa o Windows 2000 com o diretório ativo permitido.

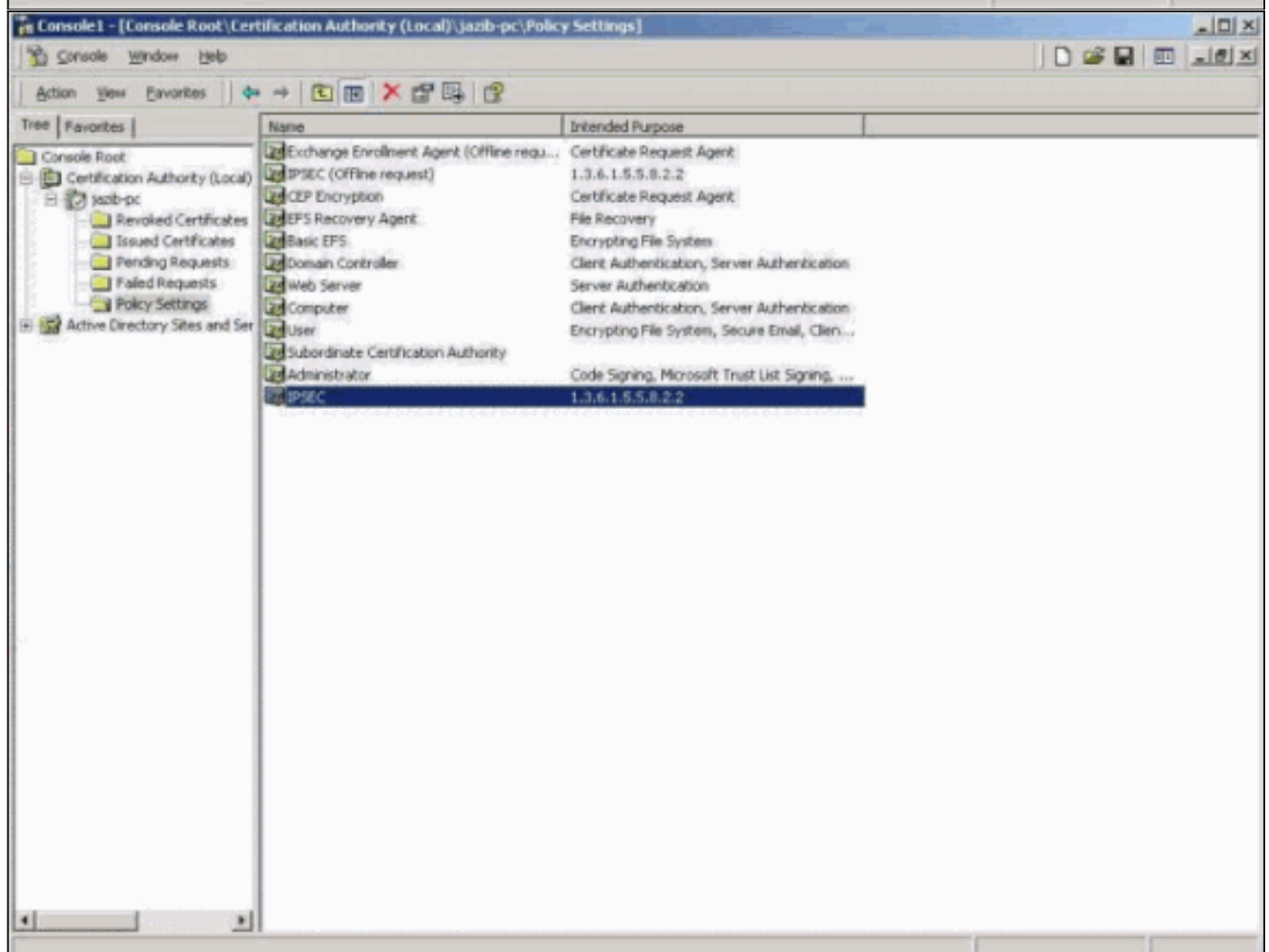
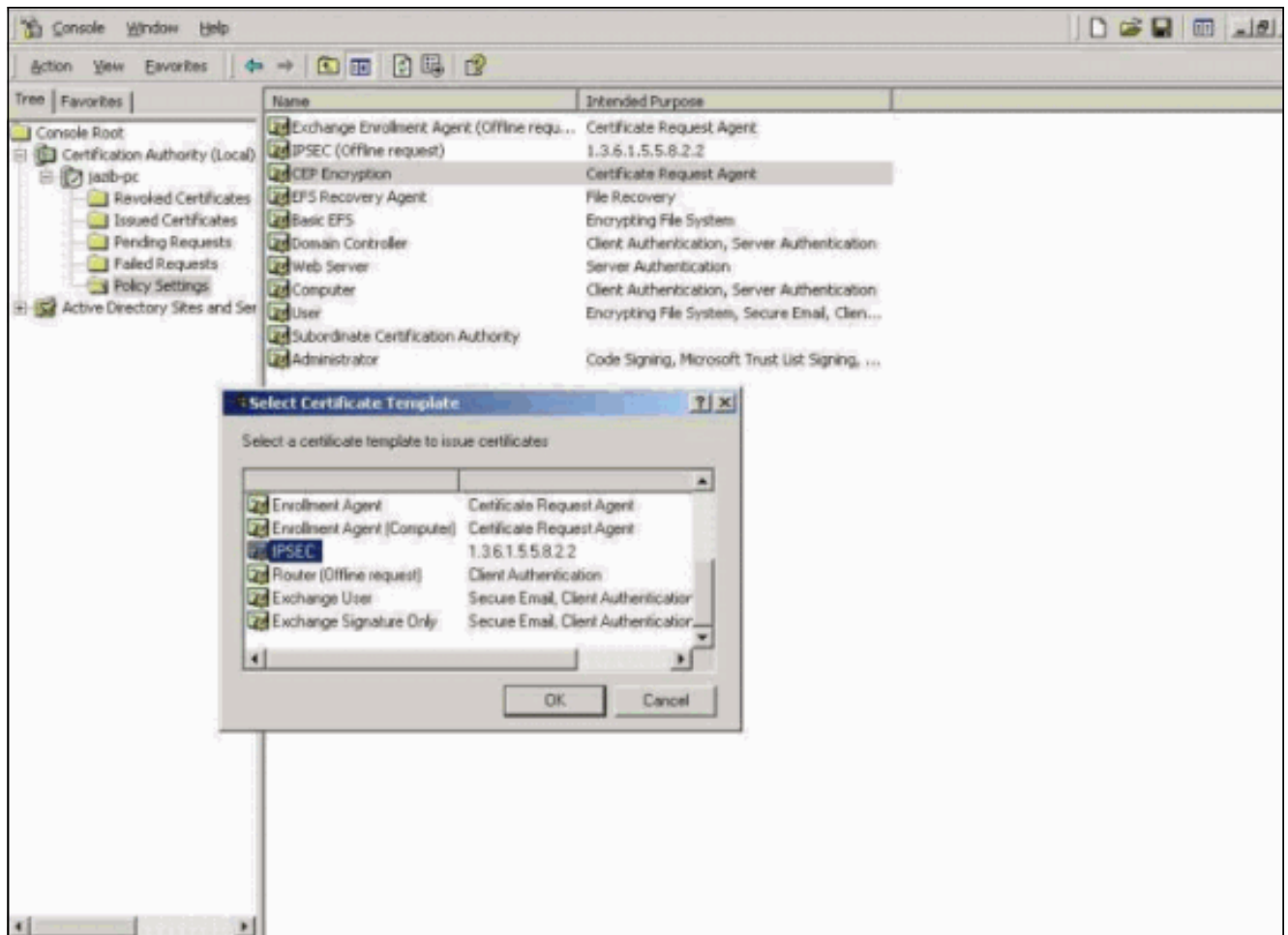
1. A fim permitir o suporte ldap no server, certifique-se de que o protocolo ldap está verificado. Conclua estes passos: Abra o Microsoft Management Console (MMC) e adicionar o **Certificate Authority**. Clicar com o botão direito o nome do servidor de CA, e clique então **propriedades**. Selecione a aba do módulo da política, e clique-a então **configuram**. Selecione a aba dos Ramais X509, e certifique-se de que somente o **LDAP** está selecionado.



2. Crie um perfil certificado novo que apoie o certificado de registro com base em arquivo no servidor certificado Empresa-baseado Windows 2000. Clicar com o botão direito **ajustes da política**, e adicionar um certificado novo para emitir. **Nota:** Se você usa um server autônomo de CA, a seguir esta etapa não é necessária.

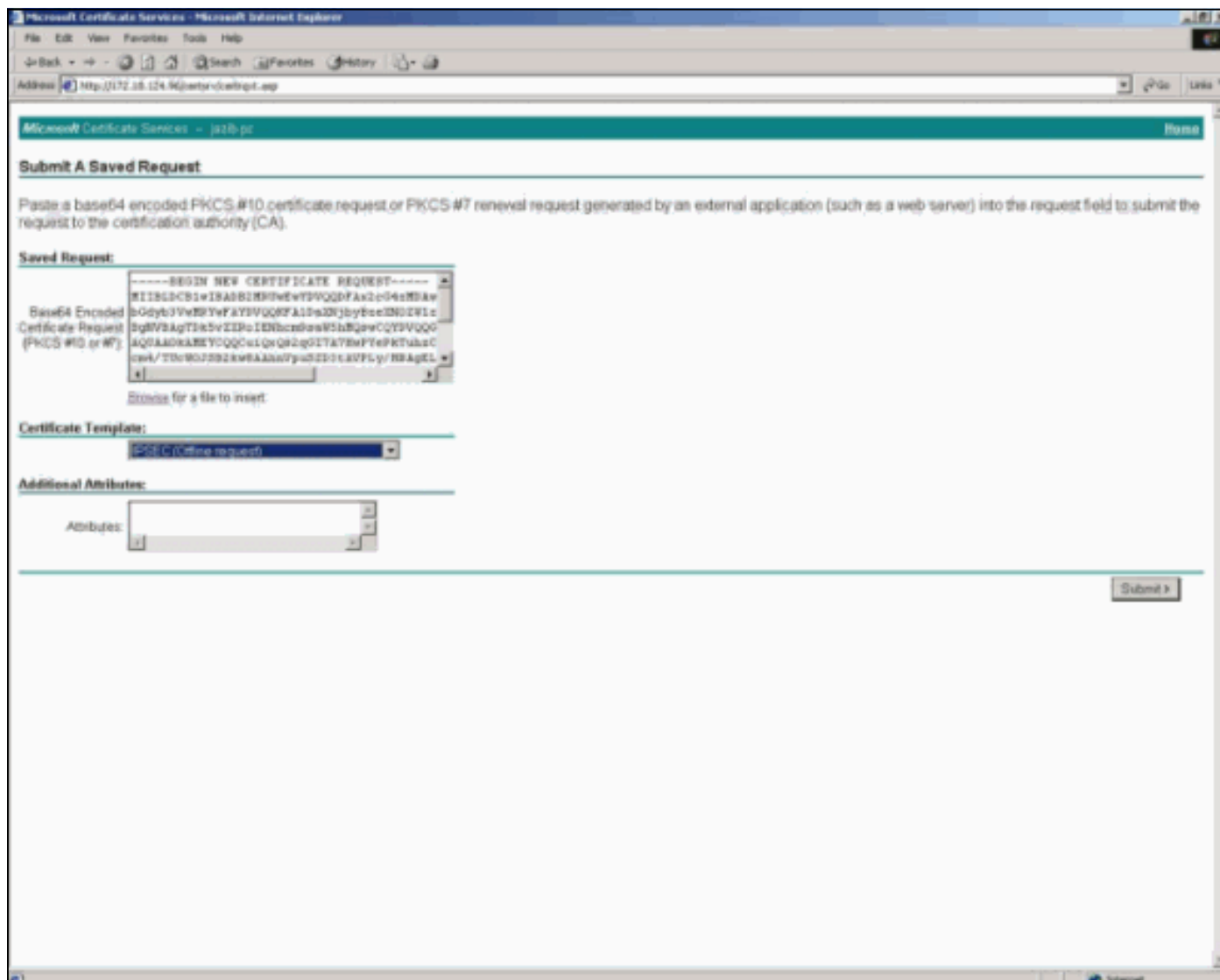


3. Adicionar o perfil certificado IPsec-baseado no servidor certificado.



## [Peça o certificado de identidade no VPN 3000 concentrator](#)

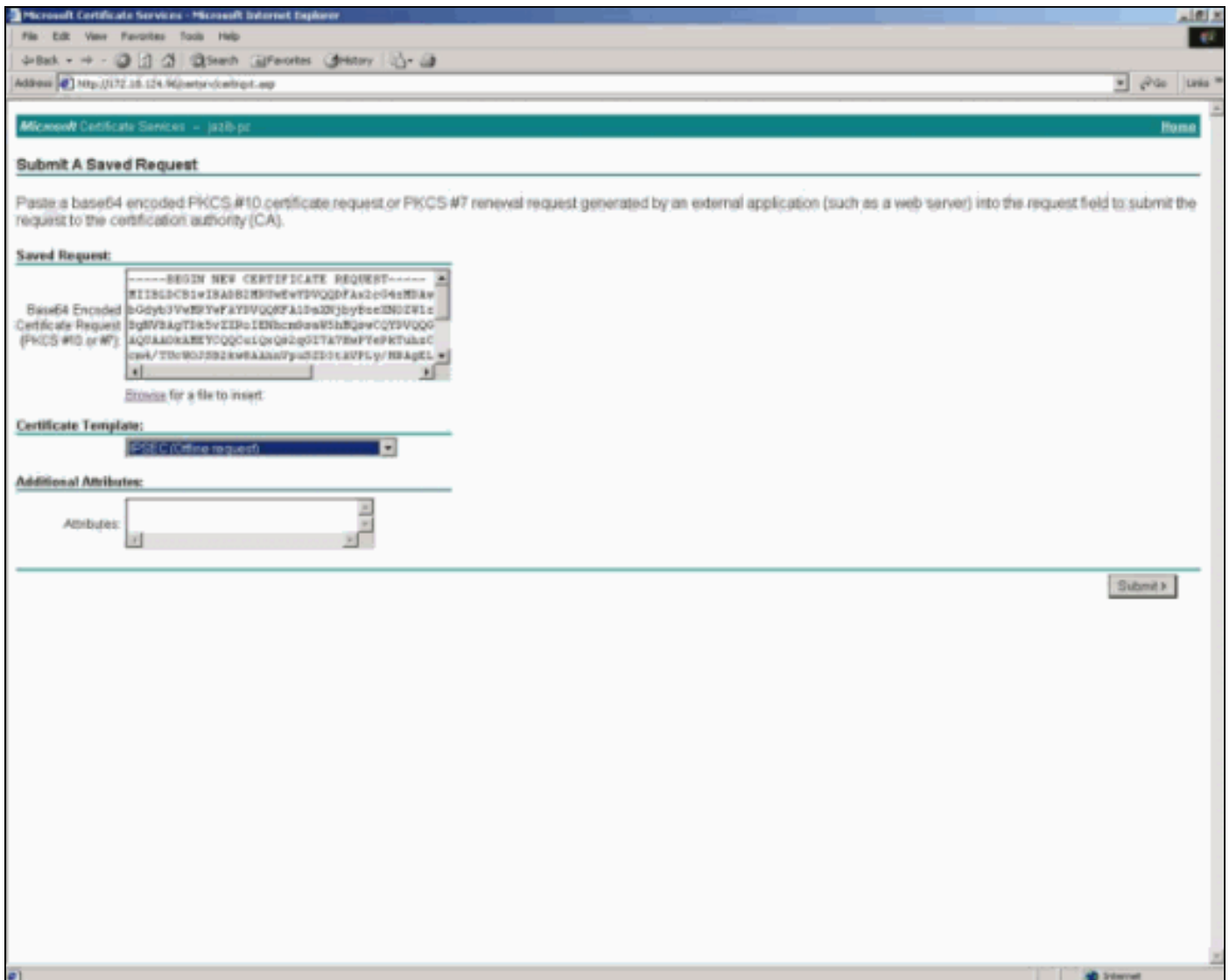
Refira [configurar o Cisco VPN 3000 Concentrator 3.0.x para obter um certificado digital](#) para obter informações sobre de como pedir um certificado de identidade. Quando você pede o certificado de identidade para o concentrador VPN, certifique-se de que você verifica o **IPSEC (pedido autônomo)** sob o molde de certificado.



The screenshot shows a web browser window titled "Microsoft Certificate Services - Microsoft Internet Explorer". The address bar shows "http://172.28.124.92/entr/cebsqt.asp". The page content includes a "Submit A Saved Request" section with instructions to paste a base64 encoded PKCS#10 certificate request or PKCS#7 renewal request. A text area contains a sample base64 encoded request: "-----BEGIN NEW CERTIFICATE REQUEST----- MIIBLjCB1wIBADBlMHQwEwYDVQQPFAs2c04cMjAkbG...". Below the text area is a "Certificate Template" dropdown menu set to "IPSEC (Offline request)". There is also an "Additional Attributes" section with an empty text box and a "Submit" button at the bottom right.

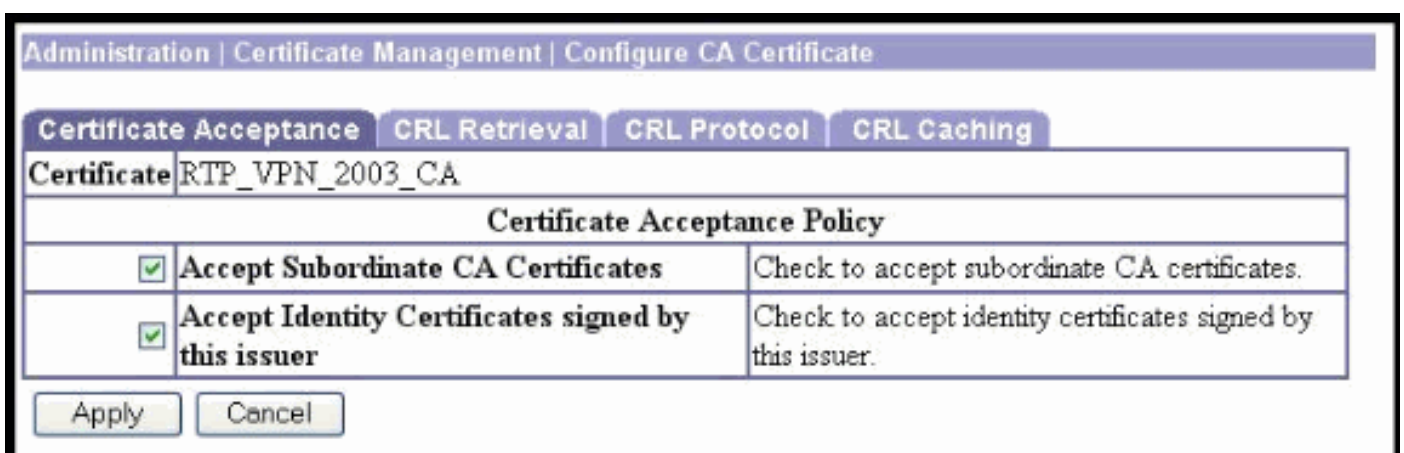
## [Peça o certificado de identidade no cliente VPN](#)

Refira [configurar o cliente VPN 3.0.x para obter um certificado digital](#) para obter informações sobre de como pedir um certificado de identidade. Quando você pede o certificado de identidade para o cliente VPN, certifique-se de que você verifica o **IPSEC (pedido autônomo)** sob o molde de certificado (como no VPN 3000 concentrator).



## [Permita o apoio CRL no VPN 3000 concentrator](#)

A fim permitir o apoio CRL no VPN 3000 concentrator, selecione o **administração > gerenciamento de certificado > os Certificados**. Clique então o **CRL** no certificado de raiz. Durante a fase 1 que processa, um par IKE pôde entregar um subordinado do certificado a este. Este certificado subordinado não pôde ser instalado no concentrador VPN. Verifique a caixa de verificação dos **certificados de CA do subordinado da aceitação** para permitir que o concentrador VPN use tais Certificados subordinados na validação de caminho do certificado. Desmarcar a caixa de verificação para recusar a característica.





Escolha a opção apropriada permitir ou desabilitar a verificação CRL em todos os Certificados emitidos por este CA. O concentrador VPN pode:

- **Use pontos estáticos da distribuição de CRL** - Use até cinco pontos estáticos da distribuição de CRL. Se você escolhe esta opção, especifique o LDAP ou os URL do HTTP na aba do protocolo de CRL.
- **Use a distribuição de CRL encaixada no certificado que é verificado** - o concentrador VPN recupera até cinco pontos da distribuição de CRL da extensão do CRL Distribution Point do certificado que é verificado e aumenta sua informação com os valores padrão configurados, caso necessário. Se a tentativa do concentrador VPN é recuperar um CRL se usando o CRL Distribution Point preliminar falha, ele experimenta de novo usando o CRL Distribution Point disponível seguinte na lista. Isto continua até que ou um CRL esteja recuperado ou a lista estiver esgotada.
- **Use os pontos da distribuição de CRL encaixados no certificado que é verificado ou então use pontos estáticos da distribuição de CRL** - se o concentrador VPN não pode encontrar cinco pontos da distribuição de CRL no certificado, adiciona pontos estáticos da distribuição de CRL, até um limite de cinco.
- **Nenhuma verificação CRL** - Não permita a verificação CRL.

Se você escolhe algumas das opções permitir a verificação CRL, configurar os protocolos de CRL em seguida na aba do protocolo de CRL.

Administration | Certificate Management | Configure CA Certificate

Certificate Acceptance | **CRL Retrieval** | CRL Protocol | CRL Caching

Certificate RTP\_VPN\_2003\_ CRL Retrieval

**CRL Retrieval Policy**

<input type="radio"/>	No CRL checking	Choose the method to use to retrieve the CRL.
<input checked="" type="radio"/>	Use static CRL distribution points	
<input type="radio"/>	Use CRL distribution points embedded in certificate being checked	
<input type="radio"/>	Use CRL distribution points embedded in certificate being checked or else use static CRL distribution points	

Apply Cancel

Escolha um protocolo do ponto de distribuição usar-se para recuperar o CRL.



Certificate Acceptance		CRL Retrieval	CRL Protocol	CRL Caching
Certificate: RTP_VPN_2003_CA				
<b>CRL Distribution Points Protocols</b>				
<input checked="" type="checkbox"/>	HTTP	Choose a distribution point protocol to use to retrieve the CRL. If you choose HTTP, be sure to assign HTTP rules to the public interface filter. (For more information, click Help.) If you choose LDAP, configure the LDAP distribution point defaults below.		
<input checked="" type="checkbox"/>	LDAP			
	Server	172.18.124.96	Enter the hostname or IP address of the server.	
	Port	389	Enter the port number of the server. The default port is 389.	
	Login DN		Enter the login DN for access to the CRL on the server.	
	Password		Enter the password for the login DN.	
	Verify		Verify the password for the login DN.	
<b>LDAP or HTTP URLs</b>				
			<ul style="list-style-type: none"> <li>• Enter up to 5 URLs to use to retrieve the CRL from the server.</li> <li>• Enter each URL on a new line.</li> </ul>	
Apply		Cancel		

## [HTTP](#)

Verifique a **caixa de verificação HTTP** para apoiar o uso do protocolo do ponto de distribuição HTTP.

**Nota:** Se você verifica o HTTP, seja certo atribuir regras HTTP ao filtro da interface pública.

## [LDAP](#)

Verifique a **caixa de verificação do LDAP** para apoiar o uso do protocolo do ponto de distribuição LDAP.

Se você escolheu apoiar pontos de distribuição LDAP, incorpore esta informação. Se a extensão do ponto de distribuição do certificado que é verificado está faltando alguns campos, o concentrador VPN usa estes valores.

- **Server** - (pontos de distribuição encaixados somente.) Entre no endereço IP ou nome do host do servidor de distribuição de CRL (servidor ldap). O máximo é 32 caracteres.
- **Porta** - (pontos de distribuição encaixados somente.) Entre no número de porta para o servidor CRL. Incorpore 0 (o padrão) para ter o fornecimento de sistema o número de porta padrão, 389 (LDAP).

## [Entre o DN](#)

Se seu server exige este campo, incorpore o início de uma sessão DN (nome destacado). O início de uma sessão DN define o caminho de diretório para alcançar este base de dados do CRL. Por exemplo, cn=crl, ou=certs, o=CANam, c=US. O comprimento de campo máximo é os caracteres 128.

## Senha

Se seu server exige uma senha para o início de uma sessão DN, incorpore-o. Os caracteres do máximo 128.

A fim verificar, reenter a senha para verificá-la. O máximo é os caracteres 128.

## LDAP ou URL do HTTP

Incorpore HTTP ou LDAP URL que identificam os CRL situados em servidores internos. Se você escolheu uma política de recuperação de CRL que use pontos de distribuição estáticos, você deve incorporar pelo menos uma (e não mais de cinco) URL válida. Incorpore cada URL em uma linha única. (Direito do rolo de incorporar valores mais longos.) Os exemplos de URL válidas são:

- URL DO HTTP: `http://1.1.1.2/CertEnroll/TestCA6-8.crl`
- LDAP URL: `jectclass=cRLDistributionPoint da chave Services,CN=Services,CN=Configuration,DC=qa2000,DC=com?certificateRevocationList?base?ob de ldap://100.199.7.6:389/CN=TestCA6-8,CN=2KPDC,CN=CDP,CN=Public`

Um administrador pode verificar a caixa de verificação **permitida** para permitir que o concentrador VPN ponha em esconderijo CRL recuperados. Este método não foi usado neste exemplo. O padrão não é permitir pôr em esconderijo CRL. O CRL de desabilitação que põe em esconderijo (que desmarca a caixa de verificação) cancela o esconderijo CRL.

Certificate	
RTP_VPN_2003_CA	
CRL Caching	
Enabled	<input type="checkbox"/> Check to enable CRL caching. Disabling will clear CRL cache.
Refresh Time	60 Enter the refresh time in minutes (5 - 1440). Enter 0 to use only the Next Update field in the cached CRL.
Enforce Next Update	<input checked="" type="checkbox"/> Check to enforce the Next Update field in CRLs. Checking this box will require valid CRLs to have a Next Update value that has not yet lapsed. Clearing the box will allow valid CRLs with no Next Update value or a Next Update value that has lapsed.
Apply Cancel	

## Horas da atualização

Especifique as horas da atualização, nos minutos, para o esconderijo CRL. A escala é 5 a 1440 minutos e o valor padrão é 60 minutos.

Incorpore 0 para usar o campo seguinte da atualização, se presente, no CRL posto em esconderijo. Se o campo seguinte da atualização não está atual no CRL, o CRL não está posto em esconderijo.

## Reforce a atualização seguinte

A característica seguinte da atualização do reforço permite que você controle como o concentrador VPN responde aos usuários que autenticam com Certificados quando o CRL associado com aqueles Certificados é antiquado.

Quando um usuário tenta autenticar com o uso de um certificado digital, o concentrador VPN

procura o CRL o mais recente associado com esse certificado. O concentrador VPN verifica o campo seguinte da atualização em seu CRL atual para determinar se um CRL mais novo pôde estar disponível. Se a próxima data da atualização é atual, o concentrador VPN usa o CRL para autenticar o usuário. Contudo, se a data decorreu, o concentrador VPN contacta o Certificate Authority para pedir um CRL mais novo.

O Certificate Authority envia um outro CRL. O CRL novo pôde ou não pôde ser mais recente. Se o campo seguinte da atualização no CRL novo é atual, o concentrador VPN usa o CRL novo para autenticar o usuário. Contudo, é possível para o Certificate Authority retornar um outro CRL com um campo seguinte antiquado da atualização. Se a próxima data da atualização neste CRL novo tem já perto, o concentrador VPN pode um ou outro uso que CRL ou não. Isto depende de como você configura a opção seguinte da atualização do reforço.

É igualmente possível que um CRL não pôde ter um campo seguinte da atualização.

Verifique a caixa de verificação **seguinte da atualização do reforço** para exigir um CRL atual. Se permitido, o concentrador VPN rejeita os CRL que não têm os campos seguintes da atualização e os CRL para que o campo seguinte da atualização decorreu.

Desmarcar a caixa se você quer o concentrador VPN poder usar os CRL sem um campo seguinte da atualização ou os CRL para que o campo seguinte da atualização decorreu.

## Debugs

Permita debuga como [configurar o VPN 3000 concentrador para comunicar-se com o cliente VPN que usa Certificados](#) descreve. Uma vez que você tem debuga permitido, se certifica de que seu debuga é similar a estes debuga.

### VPN 3000 Concentrator

```
1 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=261 172.18.124.96
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) ... total leng
th : 964
```

```
4 08/27/2001 15:24:04.680 SEV=9 IKEDBG/0 RPT=262 172.18.124.96
processing SA payload
```

```
5 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=263 172.18.124.96
Proposal # 1, Transform # 1, 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 5
Cfg'd: Oakley Group 2
```

```
10 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=264 172.18.124.96
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 5
Cfg'd: Oakley Group 1
```

```
13 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=265 172.18.124.96
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 5
```

Cfg'd: Oakley Group 1

16 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=266 172.18.124.96  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

19 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=267 172.18.124.96  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

22 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=268 172.18.124.96  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 7

25 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=269 172.18.124.96  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

28 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=270 172.18.124.96  
Proposal # 1, Transform # 2, 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 5  
Cfg'd: Oakley Group 2

33 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=271 172.18.124.96  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

36 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=272 172.18.124.96  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

39 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=273 172.18.124.96  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

42 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=274 172.18.124.96  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

45 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=275 172.18.124.96  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 7

48 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=276 172.18.124.96  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

51 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=277 172.18.124.96  
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 5  
Cfg'd: Oakley Group 2

56 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=278 172.18.124.96  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

59 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=279 172.18.124.96  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

62 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=280 172.18.124.96  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

65 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=281 172.18.124.96  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

68 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=282 172.18.124.96  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 7

71 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=283 172.18.124.96  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

74 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=284 172.18.124.96  
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 5  
Cfg'd: Oakley Group 2

79 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=285 172.18.124.96  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

82 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=286 172.18.124.96  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

85 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=287 172.18.124.96  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

88 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=288 172.18.124.96  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

91 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=289 172.18.124.96  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 7

94 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=290 172.18.124.96  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

97 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=291 172.18.124.96  
Proposal # 1, Transform # 5, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

101 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=292 172.18.124.96  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

104 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=293 172.18.124.96  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

107 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=294 172.18.124.96  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

109 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=295 172.18.124.96  
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

112 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=296 172.18.124.96  
Phase 1 failure against global IKE proposal # 6:

Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 7

115 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=297 172.18.124.96  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

117 08/27/2001 15:24:04.680 SEV=7 IKEDBG/0 RPT=298 172.18.124.96  
Oakley proposal is acceptable

118 08/27/2001 15:24:04.680 SEV=9 IKEDBG/47 RPT=7 172.18.124.96  
processing VID payload

119 08/27/2001 15:24:04.680 SEV=9 IKEDBG/49 RPT=7 172.18.124.96  
Received xauth V6 VID

120 08/27/2001 15:24:04.680 SEV=9 IKEDBG/47 RPT=8 172.18.124.96  
processing VID payload

121 08/27/2001 15:24:04.680 SEV=9 IKEDBG/49 RPT=8 172.18.124.96  
Received DPD VID

122 08/27/2001 15:24:04.680 SEV=9 IKEDBG/47 RPT=9 172.18.124.96  
processing VID payload

123 08/27/2001 15:24:04.680 SEV=9 IKEDBG/49 RPT=9 172.18.124.96  
Received Cisco Unity client VID

124 08/27/2001 15:24:04.680 SEV=9 IKEDBG/0 RPT=299 172.18.124.96  
processing IKE SA

125 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=300 172.18.124.96  
Proposal # 1, Transform # 1, 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 5  
Cfg'd: Oakley Group 2

130 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=301 172.18.124.96  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

133 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=302 172.18.124.96  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

136 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=303 172.18.124.96  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

139 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=304 172.18.124.96  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5



Cfg'd: Oakley Group 1

142 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=305 172.18.124.96  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 7

145 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=306 172.18.124.96  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

148 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=307 172.18.124.96  
Proposal # 1, Transform # 2, 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 5  
Cfg'd: Oakley Group 2

153 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=308 172.18.124.96  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

156 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=309 172.18.124.96  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

159 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=310 172.18.124.96  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

162 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=311 172.18.124.96  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

165 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=312 172.18.124.96  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 7

168 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=313 172.18.124.96  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

171 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=314 172.18.124.96  
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 5

Cfg'd: Oakley Group 2

176 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=315 172.18.124.96  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

179 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=316 172.18.124.96  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

182 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=317 172.18.124.96  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

185 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=318 172.18.124.96  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

188 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=319 172.18.124.96  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 7

191 08/27/2001 15:24:04.680 SEV=8 IKEDBG/0 RPT=320 172.18.124.96  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

194 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=321 172.18.124.96  
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 5  
Cfg'd: Oakley Group 2

199 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=322 172.18.124.96  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

202 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=323 172.18.124.96  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

205 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=324 172.18.124.96  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

208 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=325 172.18.124.96  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 1

211 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=326 172.18.124.96  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 7

214 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=327 172.18.124.96  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 5  
Cfg'd: Oakley Group 2

217 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=328 172.18.124.96  
Proposal # 1, Transform # 5, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

221 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=329 172.18.124.96  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

224 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=330 172.18.124.96  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

227 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=331 172.18.124.96  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

229 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=332 172.18.124.96  
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

232 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=333 172.18.124.96  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 7

235 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=334 172.18.124.96  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

237 08/27/2001 15:24:04.690 SEV=7 IKEDBG/28 RPT=3 172.18.124.96  
IKE SA Proposal # 1, Transform # 6 acceptable

Matches global IKE entry # 1

238 08/27/2001 15:24:04.690 SEV=8 AUTHDBG/1 RPT=7  
AUTH\_Open() returns 6

239 08/27/2001 15:24:04.690 SEV=7 AUTH/12 RPT=7  
Authentication session opened: handle = 6

240 08/27/2001 15:24:04.690 SEV=9 IKEDBG/0 RPT=335 172.18.124.96  
constructing ISA\_SA for isakmp

241 08/27/2001 15:24:04.690 SEV=8 IKEDBG/0 RPT=336 172.18.124.96  
SENDING Message (msgid=0) with payloads :  
HDR + SA (1) ... total length : 84

242 08/27/2001 15:24:04.730 SEV=8 IKEDBG/0 RPT=337 172.18.124.96  
RECEIVED Message (msgid=0) with payloads :  
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

244 08/27/2001 15:24:04.730 SEV=8 IKEDBG/0 RPT=338 172.18.124.96  
RECEIVED Message (msgid=0) with payloads :  
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

246 08/27/2001 15:24:04.730 SEV=9 IKEDBG/0 RPT=339 172.18.124.96  
processing ke payload

247 08/27/2001 15:24:04.730 SEV=9 IKEDBG/0 RPT=340 172.18.124.96  
processing ISA\_KE

248 08/27/2001 15:24:04.730 SEV=9 IKEDBG/1 RPT=41 172.18.124.96  
processing nonce payload

249 08/27/2001 15:24:04.780 SEV=9 IKEDBG/0 RPT=341 172.18.124.96  
constructing ke payload

250 08/27/2001 15:24:04.780 SEV=9 IKEDBG/1 RPT=42 172.18.124.96  
constructing nonce payload

251 08/27/2001 15:24:04.780 SEV=9 IKEDBG/46 RPT=8 172.18.124.96  
constructing Cisco Unity VID payload

252 08/27/2001 15:24:04.780 SEV=9 IKEDBG/46 RPT=9 172.18.124.96  
constructing xauth V6 VID payload

253 08/27/2001 15:24:04.780 SEV=9 IKEDBG/48 RPT=5 172.18.124.96  
Send IOS VID

254 08/27/2001 15:24:04.780 SEV=9 IKEDBG/38 RPT=3 172.18.124.96  
Constructing VPN 3000 spoofing IOS Vendor ID payload (version:  
1.0.0, capabilities: 20000001)

256 08/27/2001 15:24:04.780 SEV=9 IKEDBG/46 RPT=10 172.18.124.96  
constructing VID payload

257 08/27/2001 15:24:04.780 SEV=9 IKEDBG/48 RPT=6 172.18.124.96  
Send Altiga GW VID

258 08/27/2001 15:24:04.780 SEV=9 IKE/0 RPT=5 172.18.124.96  
Generating keys for Responder...

259 08/27/2001 15:24:04.790 SEV=8 IKEDBG/0 RPT=342 172.18.124.96  
SENDING Message (msgid=0) with payloads :  
HDR + KE (4) ... total length : 395

260 08/27/2001 15:24:04.850 SEV=8 IKEDBG/0 RPT=343 172.18.124.96  
RECEIVED Message (msgid=0) with payloads :  
HDR + ID (5) + CERT (6) + CERT\_REQ (7) + SIG (9) + NOTIFY (11) +  
NONE (0) ... total length : 1901

263 08/27/2001 15:24:04.850 SEV=9 IKEDBG/1 RPT=43 172.18.124.96  
Processing ID

264 08/27/2001 15:24:04.850 SEV=9 IKEDBG/0 RPT=344 172.18.124.96  
processing cert payload

265 08/27/2001 15:24:04.850 SEV=9 IKEDBG/0 RPT=345 172.18.124.96  
processing cert request payload

266 08/27/2001 15:24:04.850 SEV=9 IKEDBG/1 RPT=44 172.18.124.96  
processing RSA signature

267 08/27/2001 15:24:04.850 SEV=9 IKEDBG/0 RPT=346 172.18.124.96  
computing hash

268 08/27/2001 15:24:04.860 SEV=9 IKEDBG/0 RPT=347 172.18.124.96  
Processing Notify payload

269 08/27/2001 15:24:04.860 SEV=9 IKEDBG/23 RPT=3 172.18.124.96  
Starting group lookup for peer 172.18.124.96

270 08/27/2001 15:24:04.860 SEV=9 IKE/21 RPT=3 172.18.124.96  
No Group found by matching IP Address of Cert peer 172.18.124.96

271 08/27/2001 15:24:04.860 SEV=8 AUTHDBG/1 RPT=8  
AUTH\_Open() returns 7

272 08/27/2001 15:24:04.860 SEV=7 AUTH/12 RPT=8  
Authentication session opened: handle = 7

273 08/27/2001 15:24:04.860 SEV=8 AUTHDBG/3 RPT=8  
AUTH\_PutAttrTable(7, 61af64)

274 08/27/2001 15:24:04.860 SEV=8 AUTHDBG/6 RPT=3  
AUTH\_GroupAuthenticate(7, 7398828, 42dd5c)

275 08/27/2001 15:24:04.860 SEV=6 IKE/0 RPT=6  
MM received unexpected event EV\_ACTIVATE\_NEW\_SA in state  
MM\_BLD\_MSG6

276 08/27/2001 15:24:04.860 SEV=8 AUTHDBG/59 RPT=6  
AUTH\_BindServer(3ea0278, 0, 0)

277 08/27/2001 15:24:04.860 SEV=9 AUTHDBG/69 RPT=6  
Auth Server e5d99c has been bound to ACB 3ea0278, sessions = 1

278 08/27/2001 15:24:04.860 SEV=8 AUTHDBG/65 RPT=6  
AUTH\_CreateTimer(3ea0278, 0, 0)

279 08/27/2001 15:24:04.860 SEV=9 AUTHDBG/72 RPT=6  
Reply timer created: handle = 2A0017

280 08/27/2001 15:24:04.860 SEV=8 AUTHDBG/61 RPT=6  
AUTH\_BuildMsg(3ea0278, 0, 0)

281 08/27/2001 15:24:04.860 SEV=8 AUTHDBG/64 RPT=6  
AUTH\_StartTimer(3ea0278, 0, 0)

282 08/27/2001 15:24:04.860 SEV=9 AUTHDBG/73 RPT=6

Reply timer started: handle = 2A0017, timestamp = 902538,  
timeout = 30000

283 08/27/2001 15:24:04.860 SEV=8 AUTHDBG/62 RPT=6  
AUTH\_SndRequest(3ea0278, 0, 0)

284 08/27/2001 15:24:04.860 SEV=8 AUTHDBG/50 RPT=11  
IntDB\_Decode(37fc5ac, 112)

285 08/27/2001 15:24:04.860 SEV=10 AUTHDECODE/12 RPT=26  
IntDB: Type = 1 (0x01) User-Name

286 08/27/2001 15:24:04.860 SEV=10 AUTHDECODE/13 RPT=26  
IntDB: Length = 8 (0x08)

287 08/27/2001 15:24:04.860 SEV=10 AUTHDECODE/14 RPT=15  
IntDB: Value (String) =

288 08/27/2001 15:24:04.860 SEV=10 AUTHDECODE/0 RPT=15 0000: 63726C67 726F7570 crlgroup 289  
08/27/2001 15:24:04.860 SEV=10 AUTHDECODE/12 RPT=27 IntDB: Type = 5 (0x05) NAS-Port 290  
08/27/2001 15:24:04.860 SEV=10 AUTHDECODE/13 RPT=27 IntDB: Length = 4 (0x04) 291 08/27/2001  
15:24:04.860 SEV=10 AUTHDECODE/15 RPT=12 IntDB: Value (Integer) = 0 (0x0000) 292 08/27/2001  
15:24:04.860 SEV=10 AUTHDECODE/12 RPT=28 IntDB: Type = 6 (0x06) Service-Type 293 08/27/2001  
15:24:04.860 SEV=10 AUTHDECODE/13 RPT=28 IntDB: Length = 4 (0x04) 294 08/27/2001 15:24:04.860  
SEV=10 AUTHDECODE/15 RPT=13 IntDB: Value (Integer) = 2 (0x0002) 295 08/27/2001 15:24:04.860  
SEV=10 AUTHDECODE/12 RPT=29 IntDB: Type = 7 (0x07) Framed-Protocol 296 08/27/2001 15:24:04.860  
SEV=10 AUTHDECODE/13 RPT=29 IntDB: Length = 4 (0x04) 297 08/27/2001 15:24:04.860 SEV=10  
AUTHDECODE/15 RPT=14 IntDB: Value (Integer) = 1 (0x0001) 298 08/27/2001 15:24:04.860 SEV=10  
AUTHDECODE/12 RPT=30 IntDB: Type = 66 (0x42) Tunnel-Client-Endpoint 299 08/27/2001 15:24:04.860  
SEV=10 AUTHDECODE/13 RPT=30 IntDB: Length = 13 (0x0D) 300 08/27/2001 15:24:04.860 SEV=10  
AUTHDECODE/14 RPT=16 IntDB: Value (String) = 301 08/27/2001 15:24:04.860 SEV=10 AUTHDECODE/0  
RPT=16 0000: 3137322E 31382E31 32342E39 36 172.18.124.96 302 08/27/2001 15:24:04.860 SEV=10  
AUTHDECODE/12 RPT=31 IntDB: Type = 4118 (0x1016) Authentication-Server-Type 303 08/27/2001  
15:24:04.860 SEV=10 AUTHDECODE/13 RPT=31 IntDB: Length = 4 (0x04) 304 08/27/2001 15:24:04.860  
SEV=10 AUTHDECODE/15 RPT=15 IntDB: Value (Integer) = 5 (0x0005) 305 08/27/2001 15:24:04.860  
SEV=8 AUTHDBG/47 RPT=11 IntDB\_Xmt(3ea0278) 306 08/27/2001 15:24:04.860 SEV=9 AUTHDBG/71 RPT=6  
xmit\_cnt = 1 307 08/27/2001 15:24:04.860 SEV=8 AUTHDBG/47 RPT=12 IntDB\_Xmt(3ea0278) 308  
08/27/2001 15:24:04.960 SEV=8 AUTHDBG/49 RPT=6 IntDB\_Match(3ea0278, 1ff6140) 309 08/27/2001  
15:24:04.960 SEV=8 AUTHDBG/63 RPT=6 AUTH\_RcvReply(3ea0278, 0, 0) 310 08/27/2001 15:24:04.960  
SEV=8 AUTHDBG/50 RPT=12 IntDB\_Decode(1ff6140, 42) 311 08/27/2001 15:24:04.960 SEV=10  
AUTHDECODE/12 RPT=32 IntDB: Type = 1 (0x01) User-Name 312 08/27/2001 15:24:04.960 SEV=10  
AUTHDECODE/13 RPT=32 IntDB: Length = 8 (0x08) 313 08/27/2001 15:24:04.960 SEV=10 AUTHDECODE/14  
RPT=17 IntDB: Value (String) = 314 08/27/2001 15:24:04.960 SEV=10 AUTHDECODE/0 RPT=17 0000:  
63726C67 726F7570 crlgroup 315 08/27/2001 15:24:04.960 SEV=8 AUTHDBG/48 RPT=6 IntDB\_Rcv(3ea0278)  
316 08/27/2001 15:24:04.960 SEV=8 AUTHDBG/66 RPT=6 AUTH\_DeleteTimer(3ea0278, 0, 0) 317  
08/27/2001 15:24:04.960 SEV=9 AUTHDBG/74 RPT=6 Reply timer stopped: handle = 2A0017, timestamp =  
902548 318 08/27/2001 15:24:04.960 SEV=8 AUTHDBG/58 RPT=6 AUTH\_Callback(3ea0278, 0, 0) 319  
08/27/2001 15:24:04.960 SEV=6 AUTH/39 RPT=5 172.18.124.96 Authentication successful: handle = 7,  
server = Internal, group = crlgroup 320 08/27/2001 15:24:04.960 SEV=7 IKEDBG/0 RPT=348  
172.18.124.96 Group [crlgroup] Found Phase 1 Group (crlgroup) 321 08/27/2001 15:24:04.960 SEV=8  
AUTHDBG/4 RPT=4 AUTH\_GetAttrTable(7, 61afac) 322 08/27/2001 15:24:04.960 SEV=7 IKEDBG/14 RPT=4  
172.18.124.96 Group [crlgroup] Authentication configured for Internal 323 08/27/2001  
15:24:04.960 SEV=8 AUTHDBG/2 RPT=7 AUTH\_Close(7) 324 08/27/2001 15:24:04.960 SEV=8 CERT/14 RPT=3  
CERT\_Authenticate(6, 7398828, 42722c) 325 08/27/2001 15:24:04.960 SEV=8 AUTHDBG/60 RPT=6  
AUTH\_UnbindServer(3ea0278, 0, 0) 326 08/27/2001 15:24:04.960 SEV=9 AUTHDBG/70 RPT=6 Auth Server  
e5d99c has been unbound from ACB 3ea0278, sessions = 0 327 08/27/2001 15:24:04.960 SEV=8  
AUTHDBG/10 RPT=7 AUTH\_Int\_FreeAuthCB(3ea0278) 328 08/27/2001 15:24:04.960 SEV=9 AUTHDBG/19 RPT=7  
instance = 8, clone\_instance = 0 329 08/27/2001 15:24:04.960 SEV=7 AUTH/13 RPT=7 Authentication  
session closed: handle = 7 330 08/27/2001 15:24:04.960 SEV=7 CERT/5 RPT=3 Checking revocation  
status: session = 6 331 08/27/2001 15:24:04.960 SEV=8 AUTHDBG/3 RPT=9 AUTH\_PutAttrTable(6,  
f2f754) 332 08/27/2001 15:24:04.960 SEV=8 CERT/51 RPT=3 CERT\_CheckCRLConfig(3eb7914, 0, 0) 333  
08/27/2001 15:24:04.970 SEV=7 CERT/1 RPT=3 Certificate is valid: session = 6 334 08/27/2001  
15:24:04.980 SEV=8 CERT/55 RPT=2 CERT\_CheckCache(3eb7914, 0, 0) 335 08/27/2001 15:24:04.980  
SEV=8 CERT/53 RPT=2 CERT\_OpenSession(3eb7914, 0, 0) 336 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/1

RPT=9 AUTH\_Open() returns 8 337 08/27/2001 15:24:04.980 SEV=7 AUTH/12 RPT=9 Authentication session opened: handle = 8 338 08/27/2001 15:24:04.980 SEV=8 CERT/57 RPT=2  
CERT\_SndRequest(3eb7914, 0, 0) 339 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/3 RPT=10  
AUTH\_PutAttrTable(8, f2f494) 340 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/5 RPT=2  
AUTH\_Authenticate(8, 3eb7914, 47ed40) 341 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/59 RPT=7  
AUTH\_BindServer(3ea0278, 0, 0) 342 08/27/2001 15:24:04.980 SEV=9 AUTHDBG/69 RPT=7 Auth Server f162bc has been bound to ACB 3ea0278, sessions = 1 343 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/65 RPT=7 AUTH\_CreateTimer(3ea0278, 0, 0) 344 08/27/2001 15:24:04.980 SEV=9 AUTHDBG/72 RPT=7 Reply timer created: handle = 2B0017 345 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/61 RPT=7  
AUTH\_BuildMsg(3ea0278, 0, 0) 346 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/100 RPT=1  
Ldap\_Build(3ea0278) 347 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/122 RPT=1 Ldap connecting to host 172.18.124.96:389 348 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/123 RPT=1 Ldap socket 2 connected to host 172.18.124.96 349 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/107 RPT=1 Ldap directory server 172.18.124.96 is up 350 08/27/2001 15:24:04.980 SEV=7 AUTHDBG/143 RPT=1 Ldap Lookup - 16 bytes successfully received. 351 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/106 RPT=1 Ldap bind success(f162bc) 352 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/64 RPT=7 AUTH\_StartTimer(3ea0278, 0, 0) 353 08/27/2001 15:24:04.980 SEV=9 AUTHDBG/73 RPT=7 Reply timer started: handle = 2B0017, timestamp = 902550, timeout = 30000 354 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/62 RPT=7  
AUTH\_SndRequest(3ea0278, 0, 0) 355 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/101 RPT=1  
Ldap\_Xmt(3ea0278) 356 08/27/2001 15:24:04.980 SEV=8 AUTHDBG/114 RPT=1 Ldap search: DN : CN=jazib-pc,CN=jazib-pc,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=rtp-vpn,DC=cisco,DC=com Filter : objectclass=cRLDistributionPoint Scope : LDAP\_SCOPE\_BASE 360 08/27/2001 15:24:04.980 SEV=9 AUTHDBG/71 RPT=7 xmit\_cnt = 1 361 08/27/2001 15:24:05.080 SEV=7 AUTHDBG/143 RPT=2 Ldap Lookup - 497 bytes successfully received. 362 08/27/2001 15:24:05.180 SEV=7 AUTHDBG/143 RPT=3 Ldap Lookup - 16 bytes successfully received. 363 08/27/2001 15:24:05.180 SEV=8 AUTHDBG/112 RPT=1 Ldap poll got final result 364 08/27/2001 15:24:05.180 SEV=8 AUTHDBG/103 RPT=1 Ldap\_Match(3ea0278, lfe8108), id = 0x02, rcvd = 0x02 365 08/27/2001 15:24:05.180 SEV=8 AUTHDBG/63 RPT=7 AUTH\_RcvReply(3ea0278, 0, 0) 366 08/27/2001 15:24:05.180 SEV=8 AUTHDBG/102 RPT=1 Ldap\_Rcv(3ea0278) 367 08/27/2001 15:24:05.180 SEV=12 AUTHDBG/0 RPT=1 LDAP: Number of lists = 1, Rcv data length = 326 0000: 30820142 3081ED02 0101300D 06092A86 0..B0.....0...\*. 0010: 4886F70D 01010505 00308183 3120301E H.....0..1 0. 0020: 06092A86 4886F70D 01090116 116A6672 ..\*.H.....jfr 0030: 6168696D 40636973 636F2E63 6F6D310B ahim@cisco.com1. 0040: 30090603 55040613 02555331 0B300906 0...U...US1.0.. 0050: 03550408 13024E43 310C300A 06035504 .U...NC1.0...U. 0060: 07130352 54503116 30140603 55040A13 ...RTP1.0...U... 375 08/27/2001 15:24:05.180 SEV=8 AUTHDBG/98 RPT=1 LdapApiIntClose(3ea0278) 376 08/27/2001 15:24:05.180 SEV=8 AUTHDBG/66 RPT=7 AUTH\_DeleteTimer(3ea0278, 0, 0) 377 08/27/2001 15:24:05.180 SEV=9 AUTHDBG/74 RPT=7 Reply timer stopped: handle = 2B0017, timestamp = 902570 378 08/27/2001 15:24:05.180 SEV=8 AUTHDBG/58 RPT=7 AUTH\_Callback(3ea0278, 0, 0) 379 08/27/2001 15:24:05.180 SEV=6 AUTH/4 RPT=2 Authentication successful: handle = 8, server = crl\_server, user = 380 08/27/2001 15:24:05.180 SEV=8 AUTHDBG/4 RPT=5 AUTH\_GetAttrTable(8, f395e0) 381 08/27/2001 15:24:05.180 SEV=7 CERT/7 RPT=1 Retrieved revocation list: session = 6 382 08/27/2001 15:24:05.180 SEV=8 AUTHDBG/60 RPT=7 AUTH\_UnbindServer(3ea0278, 0, 0) 383 08/27/2001 15:24:05.180 SEV=9 AUTHDBG/70 RPT=7 Auth Server f162bc has been unbound from ACB 3ea0278, sessions = 0 384 08/27/2001 15:24:05.180 SEV=8 CERT/58 RPT=1 CERT\_RcvReply(3eb7914, 0, 0) 385 08/27/2001 15:24:05.180 SEV=8 CERT/54 RPT=2 CERT\_CloseSession(3eb7914, 0, 0) 386 08/27/2001 15:24:05.180 SEV=8 AUTHDBG/2 RPT=8 AUTH\_Close(8) 387 08/27/2001 15:24:05.180 SEV=8 CERT/52 RPT=1 CERT\_CheckCRL(3eb7914, 0, 0) 388 08/27/2001 15:24:05.180 SEV=8 AUTHDBG/10 RPT=8 AUTH\_Int\_FreeAuthCB(3ea0278) 389 08/27/2001 15:24:05.180 SEV=9 AUTHDBG/19 RPT=8 instance = 9, clone\_instance = 0 390 08/27/2001 15:24:05.180 SEV=7 AUTH/13 RPT=8 Authentication session closed: handle = 8 391 08/27/2001 15:24:05.180 SEV=7 CERT/2 RPT=1 Certificate has not been revoked: session = 6 392 08/27/2001 15:24:05.180 SEV=8 CERT/56 RPT=3 CERT\_Callback(3eb7914, 0, 0) 393 08/27/2001 15:24:05.180 SEV=5 IKEDBG/79 RPT=2 172.18.124.96 Group [crlgroup] Validation of certificate successful (CN=user1, SN=61A1D542000000000009) 395 08/27/2001 15:24:05.180 SEV=7 IKEDBG/0 RPT=349 172.18.124.96 Group [crlgroup] peer ID type 9 received (DER\_ASN1\_DN) 396 08/27/2001 15:24:05.190 SEV=9 IKEDBG/1 RPT=45 172.18.124.96 Group [crlgroup] constructing ID 397 08/27/2001 15:24:05.190 SEV=9 IKEDBG/0 RPT=350 172.18.124.96 Group [crlgroup] constructing cert payload 398 08/27/2001 15:24:05.190 SEV=9 IKEDBG/1 RPT=46 172.18.124.96 Group [crlgroup] constructing RSA signature 399 08/27/2001 15:24:05.190 SEV=9 IKEDBG/0 RPT=351 172.18.124.96 Group [crlgroup] computing hash 400 08/27/2001 15:24:05.200 SEV=9 IKEDBG/46 RPT=11 172.18.124.96 Group [crlgroup] constructing dpd vid payload 401 08/27/2001 15:24:05.200 SEV=8 IKEDBG/0 RPT=352 172.18.124.96 SENDING Message (msgid=0) with payloads : HDR + ID (5) ... total length : 1504 402 08/27/2001 15:24:05.200 SEV=9 IKEDBG/0 RPT=353 172.18.124.96 Group [crlgroup] constructing blank hash 403 08/27/2001 15:24:05.200 SEV=9 IKEDBG/0 RPT=354 172.18.124.96 Group [crlgroup] constructing qm hash 404 08/27/2001 15:24:05.200 SEV=8 IKEDBG/0 RPT=355 172.18.124.96 SENDING Message (msgid=feb4acac) with payloads : HDR + HASH



(8) ... total length : 100 406 08/27/2001 15:24:09.460 SEV=8 IKEDBG/0 RPT=356 172.18.124.96  
RECEIVED Message (msgid=feb4acac) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) ...  
total length : 85 408 08/27/2001 15:24:09.460 SEV=9 IKEDBG/1 RPT=47 process\_attr(): Enter! 409  
08/27/2001 15:24:09.460 SEV=9 IKEDBG/1 RPT=48 Processing cfg reply attributes. 410 08/27/2001  
15:24:09.460 SEV=8 AUTHDBG/1 RPT=10 AUTH\_Open() returns 9 411 08/27/2001 15:24:09.460 SEV=7  
AUTH/12 RPT=10 Authentication session opened: handle = 9 412 08/27/2001 15:24:09.460 SEV=8  
AUTHDBG/3 RPT=11 AUTH\_PutAttrTable(9, 61af64) 413 08/27/2001 15:24:09.460 SEV=8 AUTHDBG/5 RPT=3  
AUTH\_Authenticate(9, 2flb9a0, 45d68c) 414 08/27/2001 15:24:09.460 SEV=8 AUTHDBG/59 RPT=8  
AUTH\_BindServer(3eb81a4, 0, 0) 415 08/27/2001 15:24:09.460 SEV=9 AUTHDBG/69 RPT=8 Auth Server  
e5d99c has been bound to ACB 3eb81a4, sessions = 1 416 08/27/2001 15:24:09.460 SEV=8 AUTHDBG/65  
RPT=8 AUTH\_CreateTimer(3eb81a4, 0, 0) 417 08/27/2001 15:24:09.460 SEV=9 AUTHDBG/72 RPT=8 Reply  
timer created: handle = 2D0017 418 08/27/2001 15:24:09.460 SEV=8 AUTHDBG/61 RPT=8  
AUTH\_BuildMsg(3eb81a4, 0, 0) 419 08/27/2001 15:24:09.460 SEV=8 AUTHDBG/64 RPT=8  
AUTH\_StartTimer(3eb81a4, 0, 0) 420 08/27/2001 15:24:09.460 SEV=9 AUTHDBG/73 RPT=8 Reply timer  
started: handle = 2D0017, timestamp = 902998, timeout = 30000 421 08/27/2001 15:24:09.460 SEV=8  
AUTHDBG/62 RPT=8 AUTH\_SndRequest(3eb81a4, 0, 0) 422 08/27/2001 15:24:09.460 SEV=8 AUTHDBG/50  
RPT=13 IntDB\_Decode(37f8938, 101) 423 08/27/2001 15:24:09.460 SEV=10 AUTHDECODE/12 RPT=33 IntDB:  
Type = 1 (0x01) User-Name 424 08/27/2001 15:24:09.460 SEV=10 AUTHDECODE/13 RPT=33 IntDB: Length  
= 9 (0x09) 425 08/27/2001 15:24:09.460 SEV=10 AUTHDECODE/14 RPT=18 IntDB: Value (String) = 426  
08/27/2001 15:24:09.460 SEV=10 AUTHDECODE/0 RPT=18 0000: 69707365 63757365 72 ipsecuser 427  
08/27/2001 15:24:09.460 SEV=10 AUTHDECODE/12 RPT=34 IntDB: Type = 5 (0x05) NAS-Port 428  
08/27/2001 15:24:09.460 SEV=10 AUTHDECODE/13 RPT=34 IntDB: Length = 4 (0x04) 429 08/27/2001  
15:24:09.460 SEV=10 AUTHDECODE/15 RPT=16 IntDB: Value (Integer) =1003 (0x03EB) 430 08/27/2001  
15:24:09.460 SEV=10 AUTHDECODE/12 RPT=35 IntDB: Type = 6 (0x06) Service-Type 431 08/27/2001  
15:24:09.460 SEV=10 AUTHDECODE/13 RPT=35 IntDB: Length = 4 (0x04) 432 08/27/2001 15:24:09.460  
SEV=10 AUTHDECODE/15 RPT=17 IntDB: Value (Integer) = 2 (0x0002) 433 08/27/2001 15:24:09.460  
SEV=10 AUTHDECODE/12 RPT=36 IntDB: Type = 7 (0x07) Framed-Protocol 434 08/27/2001 15:24:09.460  
SEV=10 AUTHDECODE/13 RPT=36 IntDB: Length = 4 (0x04) 435 08/27/2001 15:24:09.460 SEV=10  
AUTHDECODE/15 RPT=18 IntDB: Value (Integer) = 1 (0x0001) 436 08/27/2001 15:24:09.460 SEV=10  
AUTHDECODE/12 RPT=37 IntDB: Type = 66 (0x42) Tunnel-Client-Endpoint 437 08/27/2001 15:24:09.460  
SEV=10 AUTHDECODE/13 RPT=37 IntDB: Length = 13 (0x0D) 438 08/27/2001 15:24:09.460 SEV=10  
AUTHDECODE/14 RPT=19 IntDB: Value (String) = 439 08/27/2001 15:24:09.460 SEV=10 AUTHDECODE/0  
RPT=19 0000: 3137322E 31382E31 32342E39 36 172.18.124.96 440 08/27/2001 15:24:09.460 SEV=8  
AUTHDBG/47 RPT=13 IntDB\_Xmt(3eb81a4) 441 08/27/2001 15:24:09.460 SEV=9 AUTHDBG/71 RPT=8 xmit\_cnt  
= 1 442 08/27/2001 15:24:09.460 SEV=8 AUTHDBG/47 RPT=14 IntDB\_Xmt(3eb81a4) 443 08/27/2001  
15:24:09.560 SEV=8 AUTHDBG/49 RPT=7 IntDB\_Match(3eb81a4, 2001040) 444 08/27/2001 15:24:09.560  
SEV=8 AUTHDBG/63 RPT=8 AUTH\_RcvReply(3eb81a4, 0, 0) 445 08/27/2001 15:24:09.560 SEV=8 AUTHDBG/50  
RPT=14 IntDB\_Decode(2001040, 60) 446 08/27/2001 15:24:09.560 SEV=10 AUTHDECODE/12 RPT=38 IntDB:  
Type = 1 (0x01) User-Name 447 08/27/2001 15:24:09.560 SEV=10 AUTHDECODE/13 RPT=38 IntDB: Length  
= 9 (0x09) 448 08/27/2001 15:24:09.560 SEV=10 AUTHDECODE/14 RPT=20 IntDB: Value (String) = 449  
08/27/2001 15:24:09.560 SEV=10 AUTHDECODE/0 RPT=20 0000: 69707365 63757365 72 ipsecuser 450  
08/27/2001 15:24:09.560 SEV=10 AUTHDECODE/12 RPT=39 IntDB: Type = 25 (0x19) Class 451 08/27/2001  
15:24:09.560 SEV=10 AUTHDECODE/13 RPT=39 IntDB: Length = 8 (0x08) 452 08/27/2001 15:24:09.560  
SEV=10 AUTHDECODE/14 RPT=21 IntDB: Value (String) = 453 08/27/2001 15:24:09.560 SEV=10  
AUTHDECODE/0 RPT=21 0000: 63726C67 726F7570 crlgroup 454 08/27/2001 15:24:09.560 SEV=8  
AUTHDBG/48 RPT=7 IntDB\_Rcv(3eb81a4) 455 08/27/2001 15:24:09.560 SEV=8 AUTHDBG/66 RPT=8  
AUTH\_DeleteTimer(3eb81a4, 0, 0) 456 08/27/2001 15:24:09.560 SEV=9 AUTHDBG/74 RPT=8 Reply timer  
stopped: handle = 2D0017, timestamp = 903008 457 08/27/2001 15:24:09.560 SEV=8 AUTHDBG/58 RPT=8  
AUTH\_Callback(3eb81a4, 0, 0) 458 08/27/2001 15:24:09.560 SEV=6 AUTH/4 RPT=3 172.18.124.96  
Authentication successful: handle = 9, server = Internal, user = ipsecuser 459 08/27/2001  
15:24:09.560 SEV=8 AUTHDBG/3 RPT=12 AUTH\_PutAttrTable(9, f39688) 460 08/27/2001 15:24:09.560  
SEV=8 AUTHDBG/60 RPT=8 AUTH\_UnbindServer(3eb81a4, 0, 0) 461 08/27/2001 15:24:09.560 SEV=9  
AUTHDBG/70 RPT=8 Auth Server e5d99c has been unbound from ACB 3eb81a4, sessions = 0 462  
08/27/2001 15:24:09.560 SEV=8 AUTHDBG/59 RPT=9 AUTH\_BindServer(3eb81a4, 0, 0) 463 08/27/2001  
15:24:09.560 SEV=9 AUTHDBG/69 RPT=9 Auth Server e5d99c has been bound to ACB 3eb81a4, sessions =  
1 464 08/27/2001 15:24:09.560 SEV=8 AUTHDBG/65 RPT=9 AUTH\_CreateTimer(3eb81a4, 0, 0) 465  
08/27/2001 15:24:09.560 SEV=9 AUTHDBG/72 RPT=9 Reply timer created: handle = 2E0017 466  
08/27/2001 15:24:09.560 SEV=8 AUTHDBG/61 RPT=9 AUTH\_BuildMsg(3eb81a4, 0, 0) 467 08/27/2001  
15:24:09.560 SEV=8 AUTHDBG/64 RPT=9 AUTH\_StartTimer(3eb81a4, 0, 0) 468 08/27/2001 15:24:09.560  
SEV=9 AUTHDBG/73 RPT=9 Reply timer started: handle = 2E0017, timestamp = 903008, timeout = 30000  
469 08/27/2001 15:24:09.560 SEV=8 AUTHDBG/62 RPT=9 AUTH\_SndRequest(3eb81a4, 0, 0) 470 08/27/2001  
15:24:09.560 SEV=8 AUTHDBG/50 RPT=15 IntDB\_Decode(2000eb0, 42) 471 08/27/2001 15:24:09.560  
SEV=10 AUTHDECODE/12 RPT=40 IntDB: Type = 1 (0x01) User-Name 472 08/27/2001 15:24:09.560 SEV=10  
AUTHDECODE/13 RPT=40 IntDB: Length = 8 (0x08) 473 08/27/2001 15:24:09.560 SEV=10 AUTHDECODE/14

RPT=22 IntDB: Value (String) = 474 08/27/2001 15:24:09.560 SEV=10 AUTHDECODE/0 RPT=22 0000: 63726C67 726F7570 crlgroup 475 08/27/2001 15:24:09.560 SEV=8 AUTHDBG/47 RPT=15  
IntDB\_Xmt(3eb81a4) 476 08/27/2001 15:24:09.560 SEV=9 AUTHDBG/71 RPT=9 xmit\_cnt = 1 477  
08/27/2001 15:24:09.560 SEV=8 AUTHDBG/47 RPT=16 IntDB\_Xmt(3eb81a4) 478 08/27/2001 15:24:09.660  
SEV=8 AUTHDBG/49 RPT=8 IntDB\_Match(3eb81a4, 20014f0) 479 08/27/2001 15:24:09.660 SEV=8  
AUTHDBG/63 RPT=9 AUTH\_RcvReply(3eb81a4, 0, 0) 480 08/27/2001 15:24:09.660 SEV=8 AUTHDBG/50  
RPT=16 IntDB\_Decode(20014f0, 42) 481 08/27/2001 15:24:09.660 SEV=10 AUTHDECODE/12 RPT=41 IntDB:  
Type = 1 (0x01) User-Name 482 08/27/2001 15:24:09.660 SEV=10 AUTHDECODE/13 RPT=41 IntDB: Length  
= 8 (0x08) 483 08/27/2001 15:24:09.660 SEV=10 AUTHDECODE/14 RPT=23 IntDB: Value (String) = **484**  
**08/27/2001 15:24:09.660 SEV=10 AUTHDECODE/0 RPT=23 0000: 63726C67 726F7570 crlgroup** 485  
08/27/2001 15:24:09.660 SEV=8 AUTHDBG/48 RPT=8 IntDB\_Rcv(3eb81a4) 486 08/27/2001 15:24:09.660  
SEV=8 AUTHDBG/66 RPT=9 AUTH\_DeleteTimer(3eb81a4, 0, 0) 487 08/27/2001 15:24:09.660 SEV=9  
AUTHDBG/74 RPT=9 Reply timer stopped: handle = 2E0017, timestamp = 903018 488 08/27/2001  
15:24:09.660 SEV=8 AUTHDBG/58 RPT=9 AUTH\_Callback(3eb81a4, 0, 0) **489 08/27/2001 15:24:09.660**  
**SEV=6 AUTH/39 RPT=6 172.18.124.96 Authentication successful: handle = 9, server = Internal,**  
**group = crlgroup** 490 08/27/2001 15:24:09.660 SEV=8 AUTHDBG/3 RPT=13 AUTH\_PutAttrTable(9, f39688)  
491 08/27/2001 15:24:09.660 SEV=8 AUTHDBG/60 RPT=9 AUTH\_UnbindServer(3eb81a4, 0, 0) 492  
08/27/2001 15:24:09.660 SEV=9 AUTHDBG/70 RPT=9 Auth Server e5d99c has been unbound from ACB  
3eb81a4, sessions = 0 493 08/27/2001 15:24:09.660 SEV=8 AUTHDBG/59 RPT=10  
AUTH\_BindServer(3eb81a4, 0, 0) 494 08/27/2001 15:24:09.660 SEV=9 AUTHDBG/69 RPT=10 Auth Server  
e5d99c has been bound to ACB 3eb81a4, sessions = 1 495 08/27/2001 15:24:09.660 SEV=8 AUTHDBG/65  
RPT=10 AUTH\_CreateTimer(3eb81a4, 0, 0) 496 08/27/2001 15:24:09.660 SEV=9 AUTHDBG/72 RPT=10 Reply  
timer created: handle = 2F0017 497 08/27/2001 15:24:09.660 SEV=8 AUTHDBG/61 RPT=10  
AUTH\_BuildMsg(3eb81a4, 0, 0) 498 08/27/2001 15:24:09.660 SEV=8 AUTHDBG/64 RPT=10  
AUTH\_StartTimer(3eb81a4, 0, 0) 499 08/27/2001 15:24:09.660 SEV=9 AUTHDBG/73 RPT=10 Reply timer  
started: handle = 2F0017, timestamp = 903018, timeout = 30000 500 08/27/2001 15:24:09.660 SEV=8  
AUTHDBG/62 RPT=10 AUTH\_SndRequest(3eb81a4, 0, 0) 501 08/27/2001 15:24:09.660 SEV=8 AUTHDBG/50  
RPT=17 IntDB\_Decode(2000d20, 42) 502 08/27/2001 15:24:09.660 SEV=10 AUTHDECODE/12 RPT=42 IntDB:  
Type = 1 (0x01) User-Name 503 08/27/2001 15:24:09.660 SEV=10 AUTHDECODE/13 RPT=42 IntDB: Length  
= 8 (0x08) 504 08/27/2001 15:24:09.660 SEV=10 AUTHDECODE/14 RPT=24 IntDB: Value (String) = 505  
08/27/2001 15:24:09.660 SEV=10 AUTHDECODE/0 RPT=24 0000: 63726C67 726F7570 crlgroup 506  
08/27/2001 15:24:09.660 SEV=8 AUTHDBG/47 RPT=17 IntDB\_Xmt(3eb81a4) 507 08/27/2001 15:24:09.660  
SEV=9 AUTHDBG/71 RPT=10 xmit\_cnt = 1 508 08/27/2001 15:24:09.660 SEV=8 AUTHDBG/47 RPT=18  
IntDB\_Xmt(3eb81a4) 509 08/27/2001 15:24:09.760 SEV=8 AUTHDBG/49 RPT=9 IntDB\_Match(3eb81a4,  
2000eb0) 510 08/27/2001 15:24:09.760 SEV=8 AUTHDBG/63 RPT=10 AUTH\_RcvReply(3eb81a4, 0, 0) 511  
08/27/2001 15:24:09.760 SEV=8 AUTHDBG/50 RPT=18 IntDB\_Decode(2000eb0, 42) 512 08/27/2001  
15:24:09.760 SEV=10 AUTHDECODE/12 RPT=43 IntDB: Type = 1 (0x01) User-Name 513 08/27/2001  
15:24:09.760 SEV=10 AUTHDECODE/13 RPT=43 IntDB: Length = 8 (0x08) 514 08/27/2001 15:24:09.760  
SEV=10 AUTHDECODE/14 RPT=25 IntDB: Value (String) = 515 08/27/2001 15:24:09.760 SEV=10  
AUTHDECODE/0 RPT=25 0000: 63726C67 726F7570 crlgroup 516 08/27/2001 15:24:09.760 SEV=8  
AUTHDBG/48 RPT=9 IntDB\_Rcv(3eb81a4) 517 08/27/2001 15:24:09.760 SEV=8 AUTHDBG/66 RPT=10  
AUTH\_DeleteTimer(3eb81a4, 0, 0) 518 08/27/2001 15:24:09.760 SEV=9 AUTHDBG/74 RPT=10 Reply timer  
stopped: handle = 2F0017, timestamp = 903028 519 08/27/2001 15:24:09.760 SEV=8 AUTHDBG/58 RPT=10  
AUTH\_Callback(3eb81a4, 0, 0) **520 08/27/2001 15:24:09.760 SEV=6 AUTH/39 RPT=7 172.18.124.96**  
**Authentication successful: handle = 9, server = Internal, group = crlgroup** 521 08/27/2001  
15:24:09.760 SEV=8 AUTHDBG/4 RPT=6 AUTH\_GetAttrTable(9, 61afac) **522 08/27/2001 15:24:09.760**  
**SEV=7 IKEDBG/14 RPT=5 172.18.124.96 Group [crlgroup] User [ipsecuser] Authentication configured**  
**for Internal** 523 08/27/2001 15:24:09.760 SEV=8 AUTHDBG/2 RPT=9 AUTH\_Close(9) **524 08/27/2001**  
**15:24:09.760 SEV=4 IKE/52 RPT=2 172.18.124.96 Group [crlgroup] User [ipsecuser] User (ipsecuser)**  
**authenticated.** 525 08/27/2001 15:24:09.760 SEV=9 IKEDBG/0 RPT=357 172.18.124.96 Group [crlgroup]  
User [ipsecuser] constructing blank hash 526 08/27/2001 15:24:09.760 SEV=9 IKEDBG/0 RPT=358  
172.18.124.96 Group [crlgroup] User [ipsecuser] constructing qm hash 527 08/27/2001 15:24:09.760  
SEV=8 IKEDBG/0 RPT=359 172.18.124.96 SENDING Message (msgid=bf771120) with payloads : HDR + HASH  
(8) ... total length : 60 529 08/27/2001 15:24:09.760 SEV=8 AUTHDBG/60 RPT=10  
AUTH\_UnbindServer(3eb81a4, 0, 0) 530 08/27/2001 15:24:09.760 SEV=9 AUTHDBG/70 RPT=10 Auth Server  
e5d99c has been unbound from ACB 3eb81a4, sessions = 0 531 08/27/2001 15:24:09.760 SEV=8  
AUTHDBG/10 RPT=9 AUTH\_Int\_FreeAuthCB(3eb81a4) 532 08/27/2001 15:24:09.760 SEV=9 AUTHDBG/19 RPT=9  
instance = 10, clone\_instance = 0 533 08/27/2001 15:24:09.760 SEV=7 AUTH/13 RPT=9 Authentication  
session closed: handle = 9 534 08/27/2001 15:24:09.770 SEV=8 IKEDBG/0 RPT=360 172.18.124.96  
RECEIVED Message (msgid=bf771120) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) ...  
total length : 56 536 08/27/2001 15:24:09.770 SEV=9 IKEDBG/1 RPT=49 process\_attr(): Enter! 537  
08/27/2001 15:24:09.770 SEV=9 IKEDBG/1 RPT=50 Processing cfg ACK attributes 538 08/27/2001  
15:24:09.770 SEV=8 IKEDBG/0 RPT=361 172.18.124.96 RECEIVED Message (msgid=826be32d) with  
payloads : HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 142 540 08/27/2001

15:24:09.770 SEV=9 IKEDBG/1 RPT=51 process\_attr(): Enter! 541 08/27/2001 15:24:09.770 SEV=9  
IKEDBG/1 RPT=52 Processing cfg Request attributes 542 08/27/2001 15:24:09.770 SEV=9 IKEDBG/1  
RPT=53 Received IPV4 address request! 543 08/27/2001 15:24:09.770 SEV=9 IKEDBG/1 RPT=54 Received  
IPV4 net mask request! 544 08/27/2001 15:24:09.770 SEV=9 IKEDBG/1 RPT=55 Received DNS server  
address request! 545 08/27/2001 15:24:09.770 SEV=9 IKEDBG/1 RPT=56 Received WINS server address  
request! 546 08/27/2001 15:24:09.770 SEV=6 IKE/130 RPT=3 172.18.124.96 Group [crlgroup] User  
[ipsecuser] Received unsupported transaction mode attribute: 5 548 08/27/2001 15:24:09.770 SEV=6  
IKE/130 RPT=4 172.18.124.96 Group [crlgroup] User [ipsecuser] Received unsupported transaction  
mode attribute: 7 550 08/27/2001 15:24:09.770 SEV=9 IKEDBG/1 RPT=57 Received Banner request! 551  
08/27/2001 15:24:09.770 SEV=9 IKEDBG/1 RPT=58 Received Save PW request! 552 08/27/2001  
15:24:09.770 SEV=9 IKEDBG/1 RPT=59 Received Default Domain request! 553 08/27/2001 15:24:09.770  
SEV=9 IKEDBG/1 RPT=60 Received Split Tunnel Include request! 554 08/27/2001 15:24:09.770 SEV=9  
IKEDBG/1 RPT=61 Received PFS request! 555 08/27/2001 15:24:09.770 SEV=4 IKE/131 RPT=2  
172.18.124.96 Group [crlgroup] User [ipsecuser] Received unknown transaction mode attribute:  
28680 557 08/27/2001 15:24:09.770 SEV=9 IKEDBG/1 RPT=62 Received UDP Port request! 558  
08/27/2001 15:24:09.770 SEV=9 IKEDBG/31 RPT=2 172.18.124.96 Group [crlgroup] User [ipsecuser]  
Obtained IP addr (10.10.10.1) prior to initiating Mode Cfg (XAuth enabled) 560 08/27/2001  
15:24:09.770 SEV=9 IKEDBG/0 RPT=362 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing  
blank hash 561 08/27/2001 15:24:09.770 SEV=9 IKEDBG/0 RPT=363 172.18.124.96 0000: 00010004  
0A0A0A01 F0010000 F0070000 ..... 562 08/27/2001 15:24:09.770 SEV=9 IKEDBG/0 RPT=364  
172.18.124.96 Group [crlgroup] User [ipsecuser] constructing qm hash 563 08/27/2001 15:24:09.770  
SEV=8 IKEDBG/0 RPT=365 172.18.124.96 SENDING Message (msgid=826be32d) with payloads : HDR + HASH  
(8) ... total length : 72 565 08/27/2001 15:24:09.810 SEV=9 IKEDBG/21 RPT=2 172.18.124.96 Group  
[crlgroup] User [ipsecuser] Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress 567  
08/27/2001 15:24:09.810 SEV=7 IKEDBG/22 RPT=2 172.18.124.96 Group [crlgroup] User [ipsecuser]  
Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed 569 08/27/2001 15:24:09.810  
SEV=4 IKE/119 RPT=2 172.18.124.96 Group [crlgroup] User [ipsecuser] PHASE 1 COMPLETED 570  
08/27/2001 15:24:09.810 SEV=6 IKE/121 RPT=2 172.18.124.96 Keep-alive type for this connection:  
DPD 571 08/27/2001 15:24:09.810 SEV=7 IKEDBG/0 RPT=366 172.18.124.96 Group [crlgroup] User  
[ipsecuser] Starting phase 1 rekey timer: 82080000 (ms) 572 08/27/2001 15:24:09.810 SEV=4  
AUTH/21 RPT=6 User ipsecuser connected 573 08/27/2001 15:24:09.810 SEV=9 IKEDBG/0 RPT=367  
172.18.124.96 Group [crlgroup] User [ipsecuser] sending notify message 574 08/27/2001  
15:24:09.810 SEV=9 IKEDBG/0 RPT=368 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing  
blank hash 575 08/27/2001 15:24:09.810 SEV=9 IKEDBG/0 RPT=369 172.18.124.96 Group [crlgroup]  
User [ipsecuser] constructing qm hash 576 08/27/2001 15:24:09.810 SEV=8 IKEDBG/0 RPT=370  
172.18.124.96 SENDING Message (msgid=b6a9bf96) with payloads : HDR + HASH (8) ... total length :  
88 578 08/27/2001 15:24:09.810 SEV=8 IKEDBG/0 RPT=371 172.18.124.96 RECEIVED Message  
(msgid=67342bd4) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE  
(0) ... total length : 792 581 08/27/2001 15:24:09.810 SEV=9 IKEDBG/0 RPT=372 172.18.124.96  
Group [crlgroup] User [ipsecuser] processing hash 582 08/27/2001 15:24:09.810 SEV=9 IKEDBG/0  
RPT=373 172.18.124.96 Group [crlgroup] User [ipsecuser] processing SA payload 583 08/27/2001  
15:24:09.810 SEV=9 IKEDBG/1 RPT=63 172.18.124.96 Group [crlgroup] User [ipsecuser] processing  
nonce payload 584 08/27/2001 15:24:09.810 SEV=9 IKEDBG/1 RPT=64 172.18.124.96 Group [crlgroup]  
User [ipsecuser] Processing ID 585 08/27/2001 15:24:09.810 SEV=5 IKE/25 RPT=3 172.18.124.96  
Group [crlgroup] User [ipsecuser] Received remote Proxy Host data in ID Payload: Address  
10.10.10.1, Protocol 0, Port 0 588 08/27/2001 15:24:09.810 SEV=9 IKEDBG/1 RPT=65 172.18.124.96  
Group [crlgroup] User [ipsecuser] Processing ID 589 08/27/2001 15:24:09.810 SEV=5 IKE/24 RPT=2  
172.18.124.96 Group [crlgroup] User [ipsecuser] Received local Proxy Host data in ID Payload:  
Address 172.18.124.132, Protocol 0, Port 0 592 08/27/2001 15:24:09.810 SEV=8 IKEDBG/0 RPT=374 QM  
IsRekeyed old sa not found by addr 593 08/27/2001 15:24:09.810 SEV=5 IKE/66 RPT=3 172.18.124.96  
Group [crlgroup] User [ipsecuser] IKE Remote Peer configured for SA: ESP-3DES-MD5 595 08/27/2001  
15:24:09.810 SEV=9 IKEDBG/0 RPT=375 172.18.124.96 Group [crlgroup] User [ipsecuser] processing  
IPSEC SA 596 08/27/2001 15:24:09.810 SEV=8 IKEDBG/0 RPT=376 Proposal # 2, Transform # 1, Type  
ESP, Id Triple-DES Parsing received transform: Phase 2 failure: Mismatched attr types for class  
HMAC Algorithm: Rcv'd: SHA Cfg'd: MD5 600 08/27/2001 15:24:09.810 SEV=7 IKEDBG/27 RPT=3  
172.18.124.96 Group [crlgroup] User [ipsecuser] IPsec SA Proposal # 3, Transform # 1 acceptable  
602 08/27/2001 15:24:09.810 SEV=7 IKEDBG/0 RPT=377 172.18.124.96 Group [crlgroup] User  
[ipsecuser] IKE: requesting SPI! 603 08/27/2001 15:24:09.810 SEV=9 IPSECDBG/6 RPT=11 IPSEC key  
message parse - msgtype 6, len 192, vers 1, pid 00000000, seq 3, err 0, type 2, mode 0, state  
32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0,  
lifecycle 0, lifetimel 7631924, lifetime2 0, dsId 300 607 08/27/2001 15:24:09.810 SEV=9  
IPSECDBG/1 RPT=37 Processing KEY\_GETSPI msg! 608 08/27/2001 15:24:09.810 SEV=7 IPSECDBG/13 RPT=3  
Reserved SPI 52918993 609 08/27/2001 15:24:09.810 SEV=8 IKEDBG/6 RPT=3 IKE got SPI from key  
engine: SPI = 0x03277ad1 610 08/27/2001 15:24:09.810 SEV=9 IKEDBG/0 RPT=378 172.18.124.96 Group

[crlgroup] User [ipsecuser] oakley constructing quick mode 611 08/27/2001 15:24:09.810 SEV=9 IKEDBG/0 RPT=379 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing blank hash 612 08/27/2001 15:24:09.810 SEV=9 IKEDBG/0 RPT=380 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing ISA\_SA for ipsec 613 08/27/2001 15:24:09.810 SEV=5 IKE/75 RPT=3 172.18.124.96 Group [crlgroup] User [ipsecuser] Overriding Initiator's IPsec rekeying duration from 2147483 to 28800 seconds 615 08/27/2001 15:24:09.810 SEV=9 IKEDBG/1 RPT=66 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing ipsec nonce payload 616 08/27/2001 15:24:09.810 SEV=9 IKEDBG/1 RPT=67 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing proxy ID 617 08/27/2001 15:24:09.810 SEV=7 IKEDBG/0 RPT=381 172.18.124.96 Group [crlgroup] User [ipsecuser] Transmitting Proxy Id: Remote host: 10.10.10.1 Protocol 0 Port 0 Local host: 172.18.124.132 Protocol 0 Port 0 621 08/27/2001 15:24:09.810 SEV=7 IKEDBG/0 RPT=382 172.18.124.96 Group [crlgroup] User [ipsecuser] Sending RESPONDER LIFETIME notification to Initiator 623 08/27/2001 15:24:09.810 SEV=9 IKEDBG/0 RPT=383 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing qm hash 624 08/27/2001 15:24:09.820 SEV=8 IKEDBG/0 RPT=384 172.18.124.96 SENDING Message (msgid=67342bd4) with payloads : HDR + HASH (8) ... total length : 172 626 08/27/2001 15:24:09.820 SEV=8 IKEDBG/0 RPT=385 172.18.124.96 RECEIVED Message (msgid=7102b770) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 796 629 08/27/2001 15:24:09.820 SEV=9 IKEDBG/0 RPT=386 172.18.124.96 Group [crlgroup] User [ipsecuser] processing hash 630 08/27/2001 15:24:09.820 SEV=9 IKEDBG/0 RPT=387 172.18.124.96 Group [crlgroup] User [ipsecuser] processing SA payload 631 08/27/2001 15:24:09.820 SEV=9 IKEDBG/1 RPT=68 172.18.124.96 Group [crlgroup] User [ipsecuser] processing nonce payload 632 08/27/2001 15:24:09.820 SEV=9 IKEDBG/1 RPT=69 172.18.124.96 Group [crlgroup] User [ipsecuser] Processing ID 633 08/27/2001 15:24:09.820 SEV=5 IKE/25 RPT=4 172.18.124.96 Group [crlgroup] User [ipsecuser] Received remote Proxy Host data in ID Payload: Address 10.10.10.1, Protocol 0, Port 0 636 08/27/2001 15:24:09.820 SEV=9 IKEDBG/1 RPT=70 172.18.124.96 Group [crlgroup] User [ipsecuser] Processing ID 637 08/27/2001 15:24:09.820 SEV=5 IKE/34 RPT=2 172.18.124.96 Group [crlgroup] User [ipsecuser] Received local IP Proxy Subnet data in ID Payload: Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0 640 08/27/2001 15:24:09.820 SEV=8 IKEDBG/0 RPT=388 QM IsRekeyed old sa not found by addr 641 08/27/2001 15:24:09.820 SEV=5 IKE/66 RPT=4 172.18.124.96 Group [crlgroup] User [ipsecuser] IKE Remote Peer configured for SA: ESP-3DES-MD5 643 08/27/2001 15:24:09.820 SEV=9 IKEDBG/0 RPT=389 172.18.124.96 Group [crlgroup] User [ipsecuser] processing IPSEC SA 644 08/27/2001 15:24:09.820 SEV=8 IKEDBG/0 RPT=390 Proposal # 2, Transform # 1, Type ESP, Id Triple-DES Parsing received transform: Phase 2 failure: Mismatched attr types for class HMAC Algorithm: Rcv'd: SHA Cfg'd: MD5 648 08/27/2001 15:24:09.820 SEV=7 IKEDBG/27 RPT=4 172.18.124.96 Group [crlgroup] User [ipsecuser] IPsec SA Proposal # 3, Transform # 1 acceptable 650 08/27/2001 15:24:09.820 SEV=7 IKEDBG/0 RPT=391 172.18.124.96 Group [crlgroup] User [ipsecuser] IKE: requesting SPI! 651 08/27/2001 15:24:09.820 SEV=9 IPSECDBG/6 RPT=12 IPSEC key message parse - msgtype 6, len 192, vers 1, pid 00000000, seq 4, err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 7633504, lifetime2 0, dsId 300 655 08/27/2001 15:24:09.830 SEV=9 IPSECDBG/1 RPT=38 Processing KEY\_GETSPI msg! 656 08/27/2001 15:24:09.830 SEV=7 IPSECDBG/13 RPT=4 Reserved SPI 1672252832 657 08/27/2001 15:24:09.830 SEV=8 IKEDBG/6 RPT=4 IKE got SPI from key engine: SPI = 0x63ac8da0 658 08/27/2001 15:24:09.830 SEV=9 IKEDBG/0 RPT=392 172.18.124.96 Group [crlgroup] User [ipsecuser] oakley constructing quick mode 659 08/27/2001 15:24:09.830 SEV=9 IKEDBG/0 RPT=393 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing blank hash 660 08/27/2001 15:24:09.830 SEV=9 IKEDBG/0 RPT=394 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing ISA\_SA for ipsec 661 08/27/2001 15:24:09.830 SEV=5 IKE/75 RPT=4 172.18.124.96 Group [crlgroup] User [ipsecuser] Overriding Initiator's IPsec rekeying duration from 2147483 to 28800 seconds 663 08/27/2001 15:24:09.830 SEV=9 IKEDBG/1 RPT=71 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing ipsec nonce payload 664 08/27/2001 15:24:09.830 SEV=9 IKEDBG/1 RPT=72 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing proxy ID 665 08/27/2001 15:24:09.830 SEV=7 IKEDBG/0 RPT=395 172.18.124.96 Group [crlgroup] User [ipsecuser] Transmitting Proxy Id: Remote host: 10.10.10.1 Protocol 0 Port 0 Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0 669 08/27/2001 15:24:09.830 SEV=7 IKEDBG/0 RPT=396 172.18.124.96 Group [crlgroup] User [ipsecuser] Sending RESPONDER LIFETIME notification to Initiator 671 08/27/2001 15:24:09.830 SEV=9 IKEDBG/0 RPT=397 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing qm hash 672 08/27/2001 15:24:09.830 SEV=8 IKEDBG/0 RPT=398 172.18.124.96 SENDING Message (msgid=7102b770) with payloads : HDR + HASH (8) ... total length : 176 674 08/27/2001 15:24:09.830 SEV=8 IKEDBG/0 RPT=399 172.18.124.96 RECEIVED Message (msgid=67342bd4) with payloads : HDR + HASH (8) + NONE (0) ... total length : 48 676 08/27/2001 15:24:09.830 SEV=9 IKEDBG/0 RPT=400 172.18.124.96 Group [crlgroup] User [ipsecuser] processing hash 677 08/27/2001 15:24:09.830 SEV=9 IKEDBG/0 RPT=401 172.18.124.96 Group [crlgroup] User [ipsecuser] loading all IPSEC SAs 678 08/27/2001 15:24:09.830 SEV=8 AUTHDBG/2 RPT=10 AUTH\_Close(6) 679 08/27/2001 15:24:09.830 SEV=9 IKEDBG/1 RPT=73 172.18.124.96 Group [crlgroup] User [ipsecuser] Generating Quick Mode Key! 680 08/27/2001 15:24:09.830 SEV=9

IKEDBG/1 RPT=74 172.18.124.96 Group [crlgroup] User [ipsecuser] Generating Quick Mode Key! 681  
08/27/2001 15:24:09.830 SEV=7 IKEDBG/0 RPT=402 172.18.124.96 Group [crlgroup] User [ipsecuser]  
Loading host: Dst: 172.18.124.132 Src: 10.10.10.1 683 08/27/2001 15:24:09.830 SEV=4 IKE/49 RPT=3  
172.18.124.96 Group [crlgroup] User [ipsecuser] Security negotiation complete for User  
(ipsecuser) Responder, Inbound SPI = 0x03277ad1, Outbound SPI = 0x45e0f379 686 08/27/2001  
15:24:09.830 SEV=9 IPSECDBG/6 RPT=13 IPSEC key message parse - msgtype 1, len 604, vers 1, pid  
00000000, seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0, spi 45e0f379, encrKeyLen 24,  
hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7633504, lifetime2 0, dsId 0 690  
08/27/2001 15:24:09.830 SEV=9 IPSECDBG/1 RPT=39 Processing KEY\_ADD msg! 691 08/27/2001  
15:24:09.840 SEV=9 IPSECDBG/1 RPT=40 key\_msghdr2secassoc(): Enter 692 08/27/2001 15:24:09.840  
SEV=7 IPSECDBG/1 RPT=41 No USER filter configured 693 08/27/2001 15:24:09.840 SEV=9 IPSECDBG/1  
RPT=42 KeyProcessAdd: Enter 694 08/27/2001 15:24:09.840 SEV=8 IPSECDBG/1 RPT=43 KeyProcessAdd:  
Adding outbound SA 695 08/27/2001 15:24:09.840 SEV=8 IPSECDBG/1 RPT=44 KeyProcessAdd: src  
172.18.124.132 mask 0.0.0.0, dst 10.10.10.1 mask 0.0.0.0 696 08/27/2001 15:24:09.840 SEV=8  
IPSECDBG/1 RPT=45 KeyProcessAdd: FilterIpssecAddIkeSa success 697 08/27/2001 15:24:09.840 SEV=9  
IPSECDBG/6 RPT=14 IPSEC key message parse - msgtype 3, len 326, vers 1, pid 00000000, seq 0, err  
0, type 2, mode 1, state 32, label 0, pad 0, spi 03277ad1, encrKeyLen 24, hashKeyLen 16, ivlen  
8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7631924, lifetime2 0, dsId 0 701 08/27/2001  
15:24:09.840 SEV=9 IPSECDBG/1 RPT=46 Processing KEY\_UPDATE msg! 702 08/27/2001 15:24:09.840  
SEV=9 IPSECDBG/1 RPT=47 Update inbound SA addresses 703 08/27/2001 15:24:09.840 SEV=9 IPSECDBG/1  
RPT=48 key\_msghdr2secassoc(): Enter 704 08/27/2001 15:24:09.840 SEV=7 IPSECDBG/1 RPT=49 No USER  
filter configured 705 08/27/2001 15:24:09.840 SEV=9 IPSECDBG/1 RPT=50 KeyProcessUpdate: Enter  
706 08/27/2001 15:24:09.840 SEV=8 IPSECDBG/1 RPT=51 KeyProcessUpdate: success 707 08/27/2001  
15:24:09.840 SEV=8 IKEDBG/7 RPT=3 IKE got a KEY\_ADD msg for SA: SPI = 0x45e0f379 708 08/27/2001  
15:24:09.840 SEV=8 IKEDBG/0 RPT=403 pitcher: rcv KEY\_UPDATE, spi 0x3277ad1 709 08/27/2001  
15:24:09.840 SEV=4 IKE/120 RPT=3 172.18.124.96 Group [crlgroup] User [ipsecuser] PHASE 2  
COMPLETED (msgid=67342bd4) 710 08/27/2001 15:24:09.840 SEV=8 AUTHDBG/10 RPT=10  
AUTH\_Int\_FreeAuthCB(3eb7914) 711 08/27/2001 15:24:09.840 SEV=9 AUTHDBG/19 RPT=10 instance = 7,  
clone\_instance = 0 712 08/27/2001 15:24:09.840 SEV=7 AUTH/13 RPT=10 Authentication session  
closed: handle = 6 713 08/27/2001 15:24:10.480 SEV=8 IKEDBG/0 RPT=404 172.18.124.96 RECEIVED  
Message (msgid=7102b770) with payloads : HDR + HASH (8) + NONE (0) ... total length : 48 715  
08/27/2001 15:24:10.490 SEV=9 IKEDBG/0 RPT=405 172.18.124.96 Group [crlgroup] User [ipsecuser]  
processing hash 716 08/27/2001 15:24:10.490 SEV=9 IKEDBG/0 RPT=406 172.18.124.96 Group  
[crlgroup] User [ipsecuser] loading all IPSEC SAs 717 08/27/2001 15:24:10.490 SEV=9 IKEDBG/1  
RPT=75 172.18.124.96 Group [crlgroup] User [ipsecuser] Generating Quick Mode Key! 718 08/27/2001  
15:24:10.490 SEV=9 IKEDBG/1 RPT=76 172.18.124.96 Group [crlgroup] User [ipsecuser] Generating  
Quick Mode Key! 719 08/27/2001 15:24:10.490 SEV=7 IKEDBG/0 RPT=407 172.18.124.96 Group  
[crlgroup] User [ipsecuser] Loading subnet: Dst: 0.0.0.0 mask: 0.0.0.0 Src: 10.10.10.1 721  
08/27/2001 15:24:10.490 SEV=4 IKE/49 RPT=4 172.18.124.96 Group [crlgroup] User [ipsecuser]  
Security negotiation complete for User (ipsecuser) Responder, Inbound SPI = 0x63ac8da0, Outbound  
SPI = 0x4a1a91ee 724 08/27/2001 15:24:10.490 SEV=9 IPSECDBG/6 RPT=15 IPSEC key message parse -  
msgtype 1, len 604, vers 1, pid 00000000, seq 0, err 0, type 2, mode 1, state 64, label 0, pad  
0, spi 4a1a91ee, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1  
7633504, lifetime2 0, dsId 0 728 08/27/2001 15:24:10.490 SEV=9 IPSECDBG/1 RPT=52 Processing  
KEY\_ADD msg! 729 08/27/2001 15:24:10.490 SEV=9 IPSECDBG/1 RPT=53 key\_msghdr2secassoc(): Enter  
730 08/27/2001 15:24:10.490 SEV=7 IPSECDBG/1 RPT=54 No USER filter configured 731 08/27/2001  
15:24:10.490 SEV=9 IPSECDBG/1 RPT=55 KeyProcessAdd: Enter 732 08/27/2001 15:24:10.490 SEV=8  
IPSECDBG/1 RPT=56 KeyProcessAdd: Adding outbound SA 733 08/27/2001 15:24:10.490 SEV=8 IPSECDBG/1  
RPT=57 KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, dst 10.10.10.1 mask 0.0.0.0 734  
08/27/2001 15:24:10.490 SEV=8 IPSECDBG/1 RPT=58 KeyProcessAdd: FilterIpssecAddIkeSa success 735  
08/27/2001 15:24:10.490 SEV=9 IPSECDBG/6 RPT=16 IPSEC key message parse - msgtype 3, len 326,  
vers 1, pid 00000000, seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0, spi 63ac8da0,  
encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7631924,  
lifetime2 0, dsId 0 739 08/27/2001 15:24:10.490 SEV=9 IPSECDBG/1 RPT=59 Processing KEY\_UPDATE  
msg! 740 08/27/2001 15:24:10.490 SEV=9 IPSECDBG/1 RPT=60 Update inbound SA addresses 741  
08/27/2001 15:24:10.490 SEV=9 IPSECDBG/1 RPT=61 key\_msghdr2secassoc(): Enter 742 08/27/2001  
15:24:10.490 SEV=7 IPSECDBG/1 RPT=62 No USER filter configured 743 08/27/2001 15:24:10.490 SEV=9  
IPSECDBG/1 RPT=63 KeyProcessUpdate: Enter 744 08/27/2001 15:24:10.490 SEV=8 IPSECDBG/1 RPT=64  
KeyProcessUpdate: success 745 08/27/2001 15:24:10.490 SEV=8 IKEDBG/7 RPT=4 IKE got a KEY\_ADD msg  
for SA: SPI = 0x4a1a91ee 746 08/27/2001 15:24:10.490 SEV=8 IKEDBG/0 RPT=408 pitcher: rcv  
KEY\_UPDATE, spi 0x63ac8da0 747 08/27/2001 15:24:10.490 SEV=4 IKE/120 RPT=4 172.18.124.96 Group  
[crlgroup] User [ipsecuser] PHASE 2 COMPLETED (msgid=7102b770) 748 08/27/2001 15:24:13.390 SEV=8  
IKEDBG/0 RPT=409 172.18.124.96 RECEIVED Message (msgid=75c17db8) with payloads : HDR + HASH (8)  
+ DELETE (12) + NONE (0) ... total length : 68 750 08/27/2001 15:24:13.390 SEV=9 IKEDBG/0

RPT=410 172.18.124.96 Group [crlgroup] User [ipsecuser] processing hash 751 08/27/2001  
15:24:13.390 SEV=9 IKEDBG/0 RPT=411 processing delete 752 08/27/2001 15:24:13.390 SEV=5 IKE/50  
RPT=3 172.18.124.96 Group [crlgroup] User [ipsecuser] Connection terminated for peer ipsecuser  
(Peer Terminate) Remote Proxy 10.10.10.1, Local Proxy 0.0.0.0 755 08/27/2001 15:24:13.390 SEV=7  
IKEDBG/9 RPT=3 172.18.124.96 Group [crlgroup] User [ipsecuser] IKE Deleting SA: Remote Proxy  
10.10.10.1, Local Proxy 0.0.0.0 757 08/27/2001 15:24:13.390 SEV=9 IPSECDBG/6 RPT=17 IPSEC key  
message parse - msgtype 2, len 258, vers 1, pid 00000000, seq 0, err 0, type 2, mode 0, state  
32, label 0, pad 0, spi 63ac8da0, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0,  
lifetype 0, lifetime1 7633504, lifetime2 0, dsId 0 761 08/27/2001 15:24:13.390 SEV=9 IPSECDBG/1  
RPT=65 Processing KEY\_DELETE msg! 762 08/27/2001 15:24:13.390 SEV=9 IPSECDBG/6 RPT=18 IPSEC key  
message parse - msgtype 2, len 258, vers 1, pid 00000000, seq 0, err 0, type 2, mode 0, state  
64, label 0, pad 0, spi 4ala91ee, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0,  
lifetype 0, lifetime1 7631924, lifetime2 0, dsId 0 766 08/27/2001 15:24:13.390 SEV=9 IPSECDBG/1  
RPT=66 Processing KEY\_DELETE msg! 767 08/27/2001 15:24:13.390 SEV=9 IPSECDBG/1 RPT=67  
key\_msghdr2secassoc(): Enter 768 08/27/2001 15:24:13.390 SEV=7 IPSECDBG/1 RPT=68 No USER filter  
configured 769 08/27/2001 15:24:13.390 SEV=8 IKEDBG/0 RPT=412 pitcher: received key delete msg,  
spi 0x63ac8da0 770 08/27/2001 15:24:13.390 SEV=8 IKEDBG/0 RPT=413 pitcher: received key delete  
msg, spi 0x4ala91ee 771 08/27/2001 15:24:13.400 SEV=8 IKEDBG/0 RPT=414 172.18.124.96 RECEIVED  
Message (msgid=8c5dbd18) with payloads : HDR + HASH (8) + DELETE (12) + NONE (0) ... total  
length : 68 773 08/27/2001 15:24:13.400 SEV=9 IKEDBG/0 RPT=415 172.18.124.96 Group [crlgroup]  
User [ipsecuser] processing hash 774 08/27/2001 15:24:13.400 SEV=9 IKEDBG/0 RPT=416 processing  
delete 775 08/27/2001 15:24:13.400 SEV=5 IKE/50 RPT=4 172.18.124.96 Group [crlgroup] User  
[ipsecuser] Connection terminated for peer ipsecuser (Peer Terminate) Remote Proxy 10.10.10.1,  
Local Proxy 172.18.124.132 778 08/27/2001 15:24:13.400 SEV=7 IKEDBG/9 RPT=4 172.18.124.96 Group  
[crlgroup] User [ipsecuser] IKE Deleting SA: Remote Proxy 10.10.10.1, Local Proxy 172.18.124.132  
780 08/27/2001 15:24:13.400 SEV=9 IKEDBG/0 RPT=417 172.18.124.96 Group [crlgroup] User  
[ipsecuser] IKE SA MM:17040521 rcv'd Terminate: state MM\_ACTIVE flags 0x0061f042, refcnt 1,  
tuncnt 0 783 08/27/2001 15:24:13.400 SEV=9 IKEDBG/0 RPT=418 172.18.124.96 Group [crlgroup] User  
[ipsecuser] IKE SA MM:17040521 terminating: flags 0x0061f002, refcnt 0, tuncnt 0 785 08/27/2001  
15:24:13.400 SEV=9 IKEDBG/0 RPT=419 sending delete message 786 08/27/2001 15:24:13.400 SEV=9  
IKEDBG/0 RPT=420 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing blank hash 787  
08/27/2001 15:24:13.400 SEV=9 IKEDBG/0 RPT=421 constructing delete payload 788 08/27/2001  
15:24:13.400 SEV=9 IKEDBG/0 RPT=422 172.18.124.96 Group [crlgroup] User [ipsecuser] constructing  
qm hash 789 08/27/2001 15:24:13.400 SEV=8 IKEDBG/0 RPT=423 172.18.124.96 SENDING Message  
(msgid=37dd4154) with payloads : HDR + HASH (8) ... total length : 76 791 08/27/2001  
15:24:13.400 SEV=9 IPSECDBG/6 RPT=19 IPSEC key message parse - msgtype 2, len 258, vers 1, pid  
00000000, seq 0, err 0, type 2, mode 0, state 32, label 0, pad 0, spi 03277ad1, encrKeyLen 0,  
hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 7633504, lifetime2 0, dsId 0 795  
08/27/2001 15:24:13.400 SEV=9 IPSECDBG/1 RPT=69 Processing KEY\_DELETE msg! 796 08/27/2001  
15:24:13.400 SEV=4 AUTH/27 RPT=2 10.10.10.1 User [ipsecuser] disconnected: Duration: 0:00:03  
Bytes xmt: 0 Bytes rcv: 0 Reason: User Requested 798 08/27/2001 15:24:13.400 SEV=9 IPSECDBG/6  
RPT=20 IPSEC key message parse - msgtype 2, len 258, vers 1, pid 00000000, seq 0, err 0, type 2,  
mode 0, state 64, label 0, pad 0, spi 45e0f379, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0,  
hmacAlg 0, lifetype 0, lifetime1 7631924, lifetime2 0, dsId 0 802 08/27/2001 15:24:13.400 SEV=9  
IPSECDBG/1 RPT=70 Processing KEY\_DELETE msg! 803 08/27/2001 15:24:13.400 SEV=9 IPSECDBG/1 RPT=71  
key\_msghdr2secassoc(): Enter 804 08/27/2001 15:24:13.400 SEV=7 IPSECDBG/1 RPT=72 No USER filter  
configured 805 08/27/2001 15:24:13.400 SEV=8 IKEDBG/0 RPT=424 pitcher: received key delete msg,  
spi 0x3277ad1 806 08/27/2001 15:24:13.400 SEV=8 IKEDBG/0 RPT=425 pitcher: received key delete  
msg, spi 0x45e0f379 807 08/27/2001 15:24:13.400 SEV=6 IKE/38 RPT=3 172.18.124.96 Header invalid,  
missing SA payload! (next payload = 8) 808 08/27/2001 15:40:47.290 SEV=4 AUTH/28 RPT=4  
Management user admin disconnected: duration 0:30:09 809 08/27/2001 15:44:49.770 SEV=3 HTTP/7  
RPT=3 172.18.124.96 HTTP 401 Unauthorized: Authorization Failed 810 08/27/2001 15:44:57.200  
SEV=5 AUTH/35 RPT=5 User [ admin ] attempted ADMIN logon.. ! 811 08/27/2001 15:44:57.200 SEV=4  
AUTH/21 RPT=7 User admin connected 812 08/27/2001 15:44:57.200 SEV=4 HTTP/47 RPT=5 172.18.124.96  
New administrator login: admin. 813 08/27/2001 15:51:51.510 SEV=1 REBOOT/1 RPT=1 Reboot  
scheduled immediately. 814 08/27/2001 15:51:51.510 SEV=4 AUTH/28 RPT=5 Management user admin  
disconnected: duration 0:06:54 815 08/27/2001 15:52:17.610 SEV=4 CONFIG/17 RPT=4 Done writing  
configuration file, Success. 816 08/27/2001 15:52:17.610 SEV=1 REBOOT/6 RPT=1 Rebooting VPN 3000  
Concentrator Series now. 1 08/27/2001 15:52:57.240 SEV=1 EVENT/37 RPT=1 Reset Reason : 2  
(Hardware-Reset) 2 08/27/2001 15:52:52.410 SEV=5 CAPI/7 RPT=1 CAPI - SEP Slot #1 disabled 3  
08/27/2001 15:52:56.100 SEV=4 CONFIG/15 RPT=1 READ header End not found. 4 08/27/2001  
15:52:57.280 SEV=4 HTTP/28 RPT=1 HTTP server starting. 5 08/27/2001 15:52:57.650 SEV=3 IP/1  
RPT=1 IP Interface 1 status changed to Link Up. 6 08/27/2001 15:52:57.670 SEV=3 IP/1 RPT=2 IP  
Interface 2 status changed to Link Up. 7 08/27/2001 15:52:57.960 SEV=3 IP/2 RPT=1 IP Interface 1



status changed to Link Down. 8 08/27/2001 15:52:57.960 SEV=3 IP/2 RPT=2 IP Interface 2 status changed to Link Down. 9 08/27/2001 15:52:59.960 SEV=3 IP/1 RPT=3 IP Interface 1 status changed to Link Up. 10 08/27/2001 15:53:02.680 SEV=5 SSL/5 RPT=1 SSL Initialized. 11 08/27/2001 15:53:02.680 SEV=4 TELNETDBG/1 RPT=1 Telnetd started 12 08/27/2001 15:53:02.680 SEV=4 TELNET/3 RPT=1 Telnetd server running 13 08/27/2001 15:53:02.690 SEV=8 AUTHDBG/13 RPT=1 AUTH\_MgmtInitServer(6c5800, 1501) 14 08/27/2001 15:53:02.690 SEV=8 AUTHDBG/95 RPT=1 LdapApiOpen(eee2bc) 15 08/27/2001 15:53:02.690 SEV=8 AUTHDBG/13 RPT=2 AUTH\_MgmtInitServer(6c5800, 1) 16 08/27/2001 15:53:02.690 SEV=8 AUTHDBG/8 RPT=1 AUTH\_TerminateSessions(e3599c) 17 08/27/2001 15:53:02.700 SEV=4 PPTP/25 RPT=1 Sockets listening for PPTP connections on socket 1 18 08/27/2001 15:53:02.710 SEV=7 CERT/36 RPT=1 Load trusted certificate: filename = SIGN0013.PEM 19 08/27/2001 15:53:02.730 SEV=7 CERT/37 RPT=1 Load identity certificate: filename = CERT0005.PEM 20 08/27/2001 15:53:02.810 SEV=8 AUTHDBG/44 RPT=1 IntDB\_Open(e3599c) 21 08/27/2001 15:53:02.810 SEV=4 AUTH/15 RPT=1 Server name = Internal, type = Internal, status = Active 22 08/27/2001 15:53:02.810 SEV=9 AUTHDBG/17 RPT=1 (Auth) index\_max = 2 23 08/27/2001 15:53:02.810 SEV=8 AUTHDBG/13 RPT=3 AUTH\_MgmtInitServer(6c5800, 2) 24 08/27/2001 15:53:02.810 SEV=8 AUTHDBG/8 RPT=2 AUTH\_TerminateSessions(e35b94) 25 08/27/2001 15:53:02.910 SEV=8 AUTHDBG/24 RPT=1 Radius\_Open(e35b94) 26 08/27/2001 15:53:02.910 SEV=7 AUTH/1 RPT=1 UDP socket opened: 1, server = 172.18.124.109 27 08/27/2001 15:53:02.910 SEV=7 AUTH/1 RPT=2 UDP socket opened: 1, server = 172.18.124.109 28 08/27/2001 15:53:02.910 SEV=4 AUTH/15 RPT=2 Server name = 172.18.124.109, type = RADIUS, status = Active 29 08/27/2001 15:53:02.910 SEV=9 AUTHDBG/17 RPT=2 (Auth) index\_max = 3 30 08/27/2001 15:53:03.730 SEV=4 SSH/2 RPT=1 SSH server starting. 31 08/27/2001 16:06:29.890 SEV=5 AUTH/35 RPT=1 User [ admin ] attempted ADMIN logon.. ! 32 08/27/2001 16:06:29.890 SEV=4 AUTH/21 RPT=1 User admin connected 33 08/27/2001 16:06:29.890 SEV=4 HTTP/47 RPT=1 172.18.124.96 New administrator login: admin.

## Cliente de VPN

228 16:13:15.088 08/27/01 Sev=Info/6 DIALER/0x63300002 Initiating connection. 229 16:13:15.098 08/27/01 Sev=Info/4 CM/0x63100002 Begin connection process 230 16:13:15.439 08/27/01 Sev=Info/4 CM/0x63100004 Establish secure connection using Ethernet 231 16:13:15.439 08/27/01 Sev=Info/4 CM/0x63100026 Attempt connection with server "172.18.124.132" 232 16:13:15.439 08/27/01 Sev=Info/6 IKE/0x6300003B Attempting to establish a connection with 172.18.124.132. 233 16:13:15.959 08/27/01 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK MM (SA, VID, VID, VID) to 172.18.124.132 234 16:13:15.969 08/27/01 Sev=Info/4 IPSEC/0x63700014 Deleted all keys 235 16:13:15.969 08/27/01 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.18.124.132 236 16:13:15.969 08/27/01 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK MM (SA) from 172.18.124.132 237 16:13:16.019 08/27/01 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK MM (KE, NON) to 172.18.124.132 238 16:13:16.059 08/27/01 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.18.124.132 239 16:13:16.059 08/27/01 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK MM (KE, NON, CERT\_REQ, VID, VID, VID, VID) from 172.18.124.132 240 16:13:16.059 08/27/01 Sev=Info/5 IKE/0x63000059 Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100 241 16:13:16.059 08/27/01 Sev=Info/5 IKE/0x63000001 Peer is a Cisco-Unity compliant peer 242 16:13:16.059 08/27/01 Sev=Info/5 IKE/0x63000059 Vendor ID payload = 09002689DFD6B712 243 16:13:16.059 08/27/01 Sev=Info/5 IKE/0x63000059 Vendor ID payload = 9A21C90230105BB437E5BE5FAF5229A5 244 16:13:16.059 08/27/01 Sev=Info/5 IKE/0x63000059 Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500300 245 16:13:16.109 08/27/01 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK MM \*(ID, CERT, CERT\_REQ, SIG, NOTIFY:STATUS\_INITIAL\_CONTACT) to 172.18.124.132 246 16:13:16.480 08/27/01 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.18.124.132 247 16:13:16.480 08/27/01 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK MM \*(ID, CERT, SIG, VID) from 172.18.124.132 248 16:13:16.590 08/27/01 Sev=Info/5 IKE/0x63000059 Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100 249 16:13:16.590 08/27/01 Sev=Info/5 IKE/0x63000001 Peer supports DPD 250 16:13:16.590 08/27/01 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.18.124.132 251 16:13:16.590 08/27/01 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from 172.18.124.132 252 16:13:16.590 08/27/01 Sev=Info/4 CM/0x63100015 Launch xAuth application 253 16:13:20.075 08/27/01 Sev=Info/4 CM/0x63100017 xAuth application returned 254 16:13:20.075 08/27/01 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 172.18.124.132 255 16:13:20.376 08/27/01 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.18.124.132 256 16:13:20.376 08/27/01 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from 172.18.124.132 257 16:13:20.376 08/27/01 Sev=Info/4 CM/0x6310000E Established Phase 1 SA. 1 Phase 1 SA in the system 258 16:13:20.376 08/27/01 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 172.18.124.132 259 16:13:20.376 08/27/01 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 172.18.124.132 260 16:13:20.386 08/27/01



Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.18.124.132 261 16:13:20.386  
08/27/01 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from  
172.18.124.132 262 16:13:20.386 08/27/01 Sev=Info/5 IKE/0x63000010 MODE\_CFG\_REPLY: Attribute =  
INTERNAL\_IPV4\_ADDRESS: , value = 10.10.10.1 263 16:13:20.386 08/27/01 Sev=Info/5 IKE/0x6300000D  
MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_SAVEPWD: , value = 0x00000000 264 16:13:20.386  
08/27/01 Sev=Info/5 IKE/0x6300000D MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_PFS: , value =  
0x00000000 265 16:13:20.396 08/27/01 Sev=Info/4 CM/0x63100019 Mode Config data received 266  
16:13:20.436 08/27/01 Sev=Info/5 IKE/0x63000055 Received a key request from Driver for IP  
address 172.18.124.132, GW IP = 172.18.124.132 267 16:13:20.436 08/27/01 Sev=Info/4  
IKE/0x63000013 SENDING >>> ISAKMP OAK QM \*(HASH, SA, NON, ID, ID) to 172.18.124.132 268  
16:13:20.436 08/27/01 Sev=Info/5 IKE/0x63000055 Received a key request from Driver for IP  
address 10.10.10.255, GW IP = 172.18.124.132 269 16:13:20.436 08/27/01 Sev=Info/4 IKE/0x63000013  
SENDING >>> ISAKMP OAK QM \*(HASH, SA, NON, ID, ID) to 172.18.124.132 270 16:13:20.446 08/27/01  
Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.18.124.132 271 16:13:20.446  
08/27/01 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK INFO \*(HASH,  
NOTIFY:STATUS\_RESP\_LIFETIME) from 172.18.124.132 **272 16:13:20.446 08/27/01 Sev=Info/5**  
**IKE/0x63000044 RESPONDER-LIFETIME notify has value of 86400 seconds 273 16:13:20.446 08/27/01**  
**Sev=Info/5 IKE/0x63000046 This SA has already been alive for 5 seconds, setting expiry to 86395**  
**seconds from now 274 16:13:20.446 08/27/01 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet:**  
peer = 172.18.124.132 275 16:13:20.446 08/27/01 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP  
OAK QM \*(HASH, SA, NON, ID, ID, NOTIFY:STATUS\_RESP\_LIFETIME) from 172.18.124.132 276  
16:13:20.446 08/27/01 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 28800  
seconds 277 16:13:20.446 08/27/01 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM \*(HASH) to  
172.18.124.132 278 16:13:20.446 08/27/01 Sev=Info/5 IKE/0x63000058 Loading IPsec SA (Message ID  
= 0x48935FCE OUTBOUND SPI = 0x3943F7FF INBOUND SPI = 0x65B16829) 279 16:13:20.446 08/27/01  
Sev=Info/5 IKE/0x63000025 Loaded OUTBOUND ESP SPI: 0x3943F7FF 280 16:13:20.446 08/27/01  
Sev=Info/5 IKE/0x63000026 Loaded INBOUND ESP SPI: 0x65B16829 **281 16:13:20.446 08/27/01**  
**Sev=Info/4 CM/0x6310001A One secure connection established 282 16:13:20.496 08/27/01 Sev=Info/6**  
**DIALER/0x63300003 Connection established. 283 16:13:20.556 08/27/01 Sev=Info/6 DIALER/0x63300008**  
MAPI32 Information - Outlook not default mail client 284 16:13:21.097 08/27/01 Sev=Info/5  
IKE/0x6300002F Received ISAKMP packet: peer = 172.18.124.132 285 16:13:21.097 08/27/01  
Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK QM \*(HASH, SA, NON, ID, ID,  
NOTIFY:STATUS\_RESP\_LIFETIME) from 172.18.124.132 286 16:13:21.097 08/27/01 Sev=Info/5  
IKE/0x63000044 RESPONDER-LIFETIME notify has value of 28800 seconds 287 16:13:21.097 08/27/01  
Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM \*(HASH) to 172.18.124.132 288 16:13:21.097  
08/27/01 Sev=Info/5 IKE/0x63000058 Loading IPsec SA (Message ID = 0x1FE7AC28 OUTBOUND SPI =  
0x557D6E94 INBOUND SPI = 0x8A8A034D) 289 16:13:21.107 08/27/01 Sev=Info/5 IKE/0x63000025 Loaded  
OUTBOUND ESP SPI: 0x557D6E94 290 16:13:21.107 08/27/01 Sev=Info/5 IKE/0x63000026 Loaded INBOUND  
ESP SPI: 0x8A8A034D 291 16:13:21.107 08/27/01 Sev=Info/4 CM/0x63100022 Additional Phase 2 SA  
established. 292 16:13:21.107 08/27/01 Sev=Info/4 IPSEC/0x63700014 Deleted all keys **293**  
**16:13:21.107 08/27/01 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 294 16:13:21.107**  
**08/27/01 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0xffff74339 into key list 295**  
16:13:21.107 08/27/01 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 296 16:13:21.107  
08/27/01 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0x2968b165 into key list 297  
16:13:21.107 08/27/01 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 298 16:13:21.107  
08/27/01 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0x946e7d55 into key list 299  
16:13:21.107 08/27/01 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 300 16:13:21.107  
08/27/01 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0x4d038a8a into key list

## [Informações Relacionadas](#)

- [Página de suporte do Cisco VPN 3000 Series Concentrator](#)
- [Página de suporte ao cliente do Cisco VPN 3000 Series](#)
- [Página de suporte do IPsec](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)