

# Configurando o IPsec entre um roteador do Cisco IOS e um Cisco VPN Client 4.x para Windows usando o RADIUS

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Material de Suporte](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração de servidor RADIUS](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Saída de depurações](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento demonstra como configurar uma conexão entre um Cisco IOS Router e o Cisco VPN Client 4.x usando o RADIUS para autorização de grupo e autenticação de usuário. O Cisco IOS® Software Release 12.2(8)T ou posterior suporta conexões do Cisco VPN Client 3.x. Os VPN Clients 3.x e 4.x usam as políticas de Diffie Hellman (DH) group 2. O comando `isakmp policy # group 2` permite que os VPN Clients se conectem.

**Nota:** Explicar do IPSec VPN está agora disponível. Refira o [IPSec VPN que esclarece](#) mais configurações da informação e de amostra.

## [Pré-requisitos](#)

### [Requisitos](#)

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Um conjunto de endereços a ser atribuído ao IPSec.
- Um grupo chamado "3000clients" com uma chave pré-compartilhada de "cisco123"

- Autorização e autenticação de usuário do grupo em um servidor Radius

**Nota:** A contabilidade do RAO não é apoiada neste tempo.

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Um 2611 Router que execute o Cisco IOS Software Release 12.2(8)T.
- Cisco Secure ACS for Windows (todo o servidor Radius deve trabalhar)
- Cisco VPN Client para a versão do Windows 4.8 (todo o cliente VPN 4.x deve trabalhar)

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.

Isto output do **comando show version** no roteador:

```
vpn2611#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JK9O3S-M), Version 12.2(8)T,
  RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 14-Feb-02 16:50 by ccai
Image text-base: 0x80008070, data-base: 0x81816184

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

vpn2611 uptime is 1 hour, 15 minutes
System returned to ROM by reload
System image file is "flash:c2600-jk9o3s-mz.122-8.T"

cisco 2611 (MPC860) processor (revision 0x203)
  with 61440K/4096K bytes of memory.
Processor board ID JAD04370EEG (2285146560)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

## Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## Material de Suporte

Este documento mostra a authentication e autorização, tal como a atribuição do Windows Internet Naming Service (VITÓRIAS) e do Domain Naming Service (DNS), pelo servidor Radius. Se você

está interessado em executar a autenticação pelo servidor Radius e a autorização localmente pelo roteador, refira [configurar o IPsec entre um roteador do Cisco IOS e um Cisco VPN Client 4.x para Windows usando o RAIO para a autenticação de usuário](#).

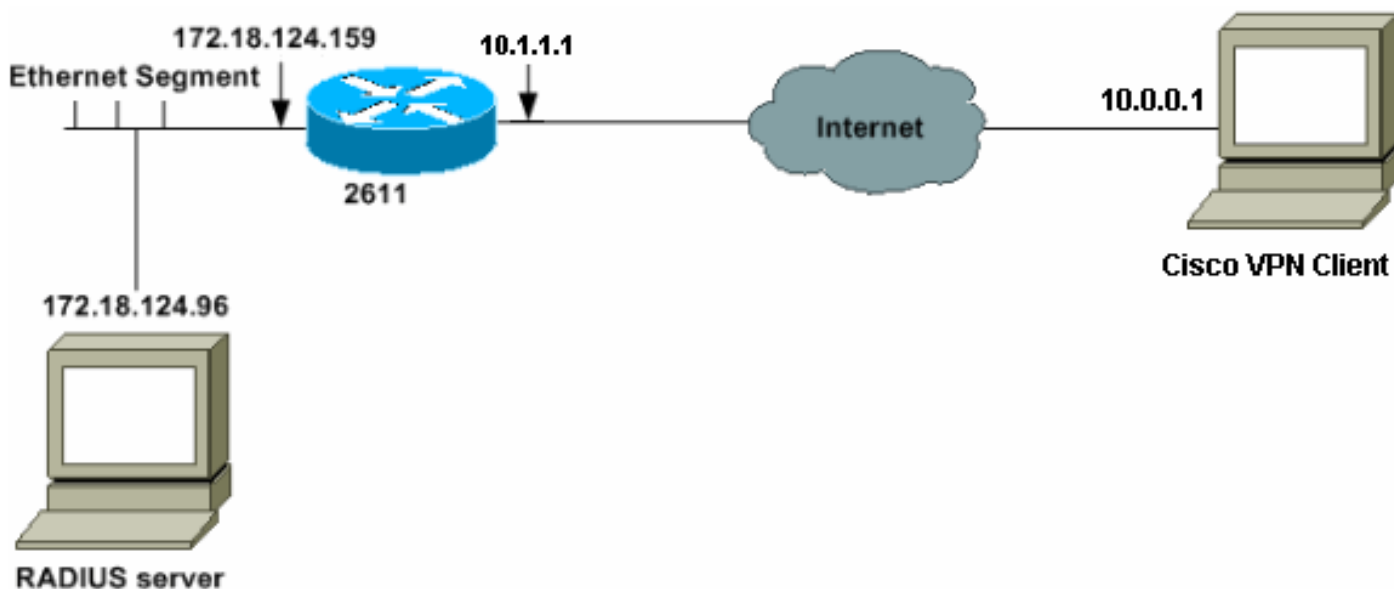
## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Nota:** Use a ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



**Nota:** Os endereços IP de Um ou Mais Servidores Cisco ICM NT nesta rede de exemplo não são roteável nos Internet globais porque são endereços IP privados em uma rede de laboratório.

## Configurações

### 2611 Router

```
vpn2611#show run
Building configuration...

Current configuration : 1884 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname vpn2611
!
!--- Enable AAA for user authentication and group
```

```

authorization. aaa new-model
!
!--- In order to enable extended authentication (Xauth)
for user authentication, !--- enable the aaa
authentication commands. !--- "Group radius" specifies
RADIUS user authentication.

aaa authentication login userauthen group radius

!--- In order to enable group authorization, !--- enable
the aaa authorization commands.

aaa authorization network groupauthor group radius
!
!
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
!--- Create an Internet Security Association and !---
Key Management Protocol (ISAKMP) policy for Phase 1
negotiations. crypto isakmp policy 3
encr 3des
authentication pre-share
group 2
!
!
!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-sha-hmac
!
!--- Create a dynamic map and !--- apply the transform
set that was created. crypto dynamic-map dynmap 10
set transform-set myset
!
!--- Create the actual crypto map, !--- and apply the
AAA lists that were created earlier. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
!--- Apply the crypto map on the outside interface.
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
half-duplex
crypto map clientmap
!
interface Serial0/0
no ip address
shutdown

```

```

!
interface Ethernet0/1
 ip address 172.18.124.159 255.255.255.0
 no keepalive
 half-duplex
!

!--- Create a pool of addresses to be assigned to the
VPN Clients. ip local pool ippool 10.16.20.1
10.16.20.200
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
ip http server
ip pim bidir-enable
!

!--- Create an access control list (ACL) if you want to
do split tunneling. !--- This ACL is referenced in the
RADIUS profile. access-list 108 permit ip 172.18.124.0
0.0.255.255 10.16.20.0 0.0.0.255
!

!--- Specify the IP address of the RADIUS server, !---
along with the RADIUS shared secret key. radius-server
host 172.18.124.96 auth-port 1645 acct-port 1646 key
cisco123 radius-server retransmit 3
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end

vpn2611#

```

## [Configuração de servidor RADIUS](#)

### [Configurar o servidor Radius para clientes de AAA \(o roteador\)](#)

Conclua estes passos:

1. O clique **adiciona a entrada** para adicionar o roteador à base de dados do servidor radius.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">340</a>	172.18.124.151	RADIUS (Cisco Aironet)
<a href="#">Aironet-340-Lab</a>	14.36.1.99	RADIUS (Cisco Aironet)
<a href="#">glenrtest</a>	172.18.124.120	RADIUS (Cisco IOS/PIX)
<a href="#">router</a>	172.18.124.150	TACACS+ (Cisco IOS)

2. Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT do roteador "172.18.124.159" junto com a chave secreta compartilhada "cisco123" e escolha o **RAIO** na autenticação usando a caixa suspensa.

## [Configurar o servidor Radius para a authentication e autorização do grupo](#)

Conclua estes passos:

1. O clique **adiciona/edita** para adicionar um usuário nomeado **3000client** ao servidor Radius.

2. Especifique a senha **Cisco** para este usuário. Esta senha é um palavra-chave especial para o Cisco IOS, que indique que um perfil de grupo deve ser provido. Você pode traçar o usuário a um grupo seguro de Cisco se você preferir. Certifique-se de que **nenhuma atribuição do**

endereço IP de Um ou Mais Servidores Cisco ICM NT está escolhida.

**User Setup**

Password Authentication:

CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When using a Token Card server for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Group 20

Callback:

Use group setting

No callback allowed

Callback using this number

Dialup client specifies callback number

Use Microsoft NT callback settings

Client IP Address Assignment:

Use group settings

No IP address assignment

Assigned by dialup client

Assign static IP address

Assigned by AAA client pool

Submit Delete Cancel

3. Especifique os parâmetros de autorização do grupo que serão passados para baixo por esta conta de usuário de volta ao cliente VPN. Certifique-se de que você tem o **Cisco-av-pair** permitido com estes atributos: IPsec: key-exchange=ike IPsec: key-exchange=preshared-key IPsec: addr-pool=ippool ipsec: inacl=108 (necessário somente se você usa o Split Tunneling no roteador) Também, certifique-se de que você tem atributos de raio de IETF do theseg permitidos: Atributo 6: Service-Type=Outbound Atributo 64: Tunnel-Type=IP ESP Atributo 69:

Tunnel-Password=cisco123 (este é seu group password no cliente VPN)Uma vez que você terminou, o clique **submete-se**.

Checking this option will PERMIT all UNKNOWN Services

Default (Undefined) Services

**Cisco IOS/PIX RADIUS Attributes** ?

[009\001] cisco-av-pair

```
ipsec:key-exchange=ike
ipsec:key-exchange=preshared-key
ipsec:addr-pool=ippool
ipsec:inacl=100
```

**IETF RADIUS Attributes** ?

[006] Service-Type Outbound

[007] Framed-Protocol PPP

[027] Session-Timeout 0

[028] Idle-Timeout 0

[064] Tunnel-Type

Tag 1 Value IP ESP

Tag 2 Value

[069] Tunnel-Password

Tag 1 Value cisco123

Tag 2 Value

Submit Delete Cancel


Sob atributos específicos do vendedor, você pode igualmente permitir estes atributos opcionais: IPsec: default-domain=IPsec: timeout=IPsec: idletime=IPsec: dns-servers=IPsec: wins-servers=

### [Configurar o servidor Radius para a autenticação de usuário](#)

Conclua estes passos:



1. O clique **adiciona/edita** para adicionar o usuário VPN no base de dados seguro de Cisco. Neste exemplo, o username é Cisco.

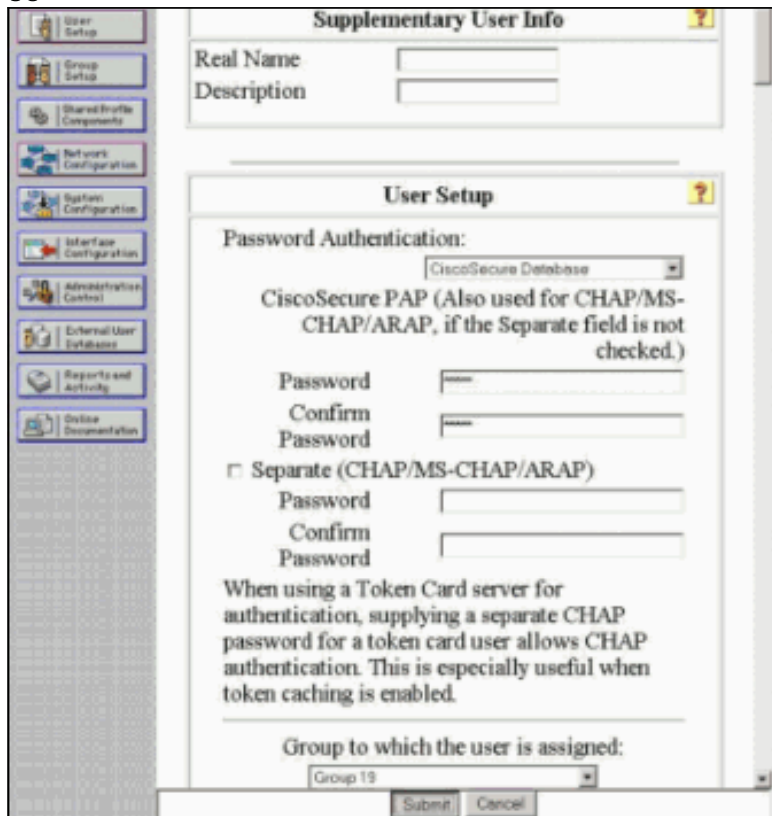


The screenshot shows the Cisco User Setup interface. On the left is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main area has a 'User:' field containing 'cisco' with 'Find' and 'Add/Edit' buttons. Below it, a list of users beginning with 'c' is shown: C, C1, C2, C3, C4, C5, C6, C7, C8, C9, C10, C11, C12, C13, C14, C15, C16, C17, C18, C19, C20, C21, C22, C23, C24, C25, C26, C27, C28, C29, C30, C31, C32, C33, C34, C35, C36, C37, C38, C39, C40, C41, C42, C43, C44, C45, C46, C47, C48, C49, C50, C51, C52, C53, C54, C55, C56, C57, C58, C59, C60, C61, C62, C63, C64, C65, C66, C67, C68, C69, C70, C71, C72, C73, C74, C75, C76, C77, C78, C79, C80, C81, C82, C83, C84, C85, C86, C87, C88, C89, C90, C91, C92, C93, C94, C95, C96, C97, C98, C99, C100. There are 'List All Users' and 'Back to Help' buttons at the bottom.

- [User Setup and External User Databases](#)
- [Finding a Specific User in the CiscoSecure User Database](#)
- [Adding a User to the CiscoSecure User Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the CiscoSecure User Database](#)
- [Changing a Username in the CiscoSecure User Database](#)

User Setup enables you to configure individual user information, add users, and delete users in the database.

2. Na próxima janela, especifique a senha para o usuário **Cisco**. A senha é igualmente **Cisco**. Você pode traçar a conta de usuário a um grupo. Uma vez que você terminou, o clique **submete-se**.



The screenshot shows the 'Supplementary User Info' and 'User Setup' sections. The 'Supplementary User Info' section has fields for 'Real Name' and 'Description'. The 'User Setup' section has a 'Password Authentication:' dropdown set to 'CiscoSecure Database'. Below it, there are fields for 'Password' and 'Confirm Password' for the main authentication, and another set for 'Separate (CHAP/MS-CHAP/ARAP)' authentication. A note explains that a separate CHAP password is useful for token card users. At the bottom, there is a 'Group to which the user is assigned:' dropdown set to 'Group 19' and 'Submit' and 'Cancel' buttons.

- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

**Account Disabled Status**

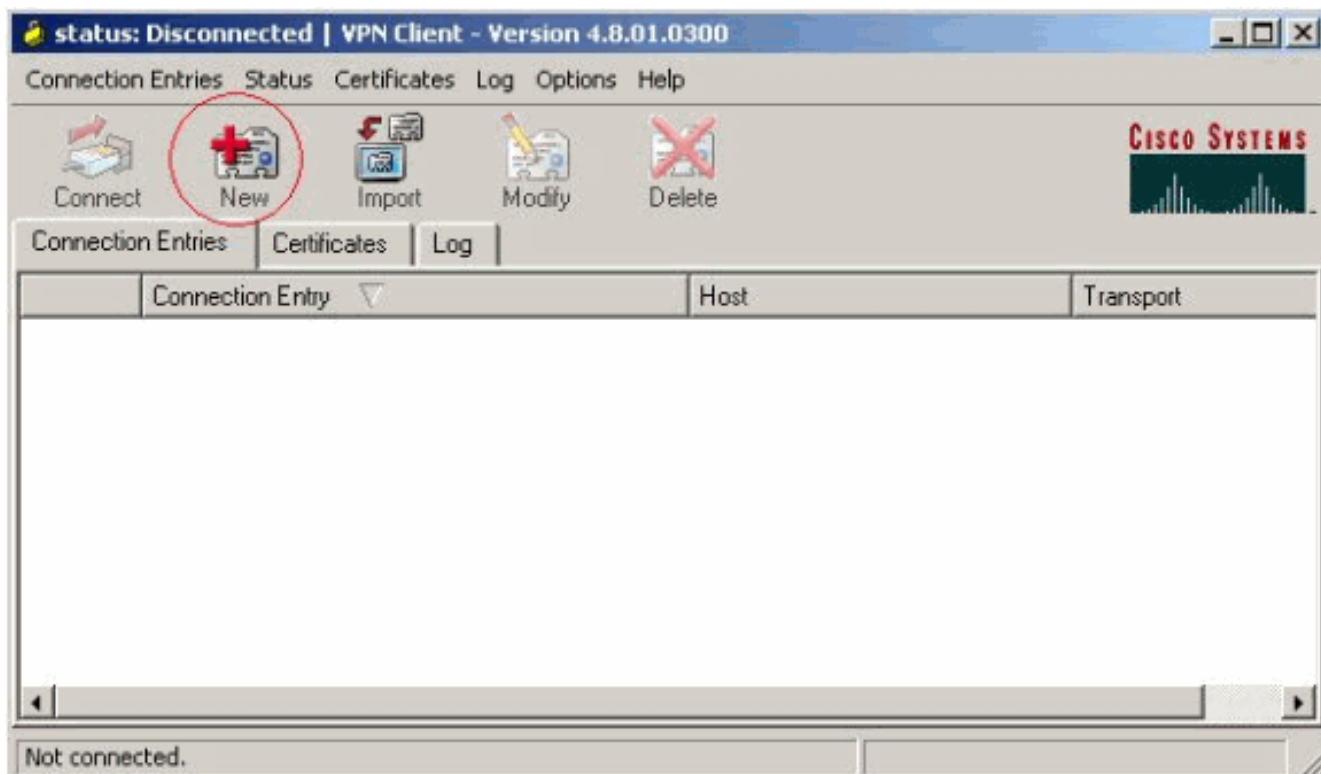
Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[\[Back to Top\]](#)

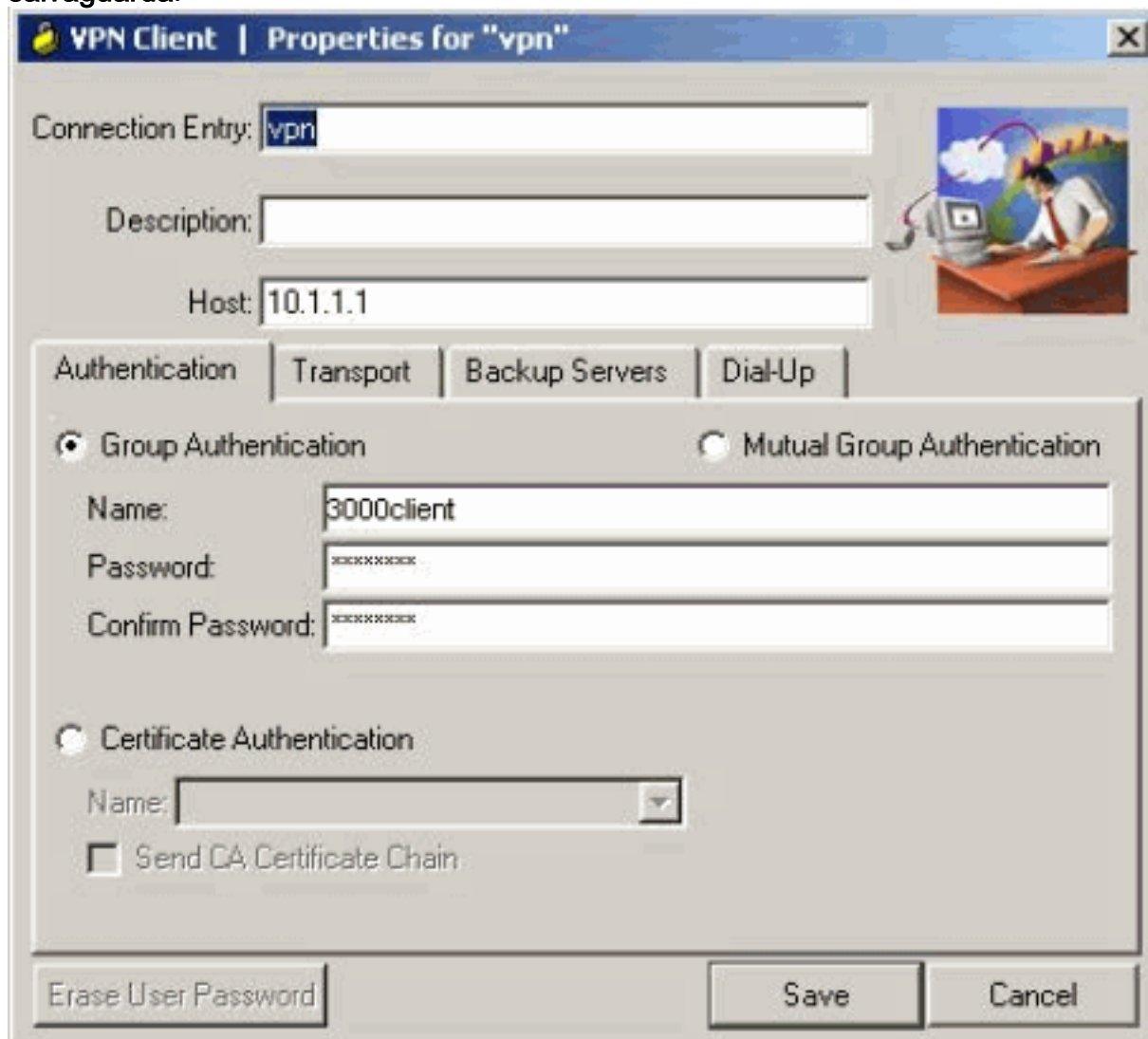
## [Configuração do cliente VPN 4.8](#)

Termine estas etapas a fim configurar o cliente VPN 4.8:

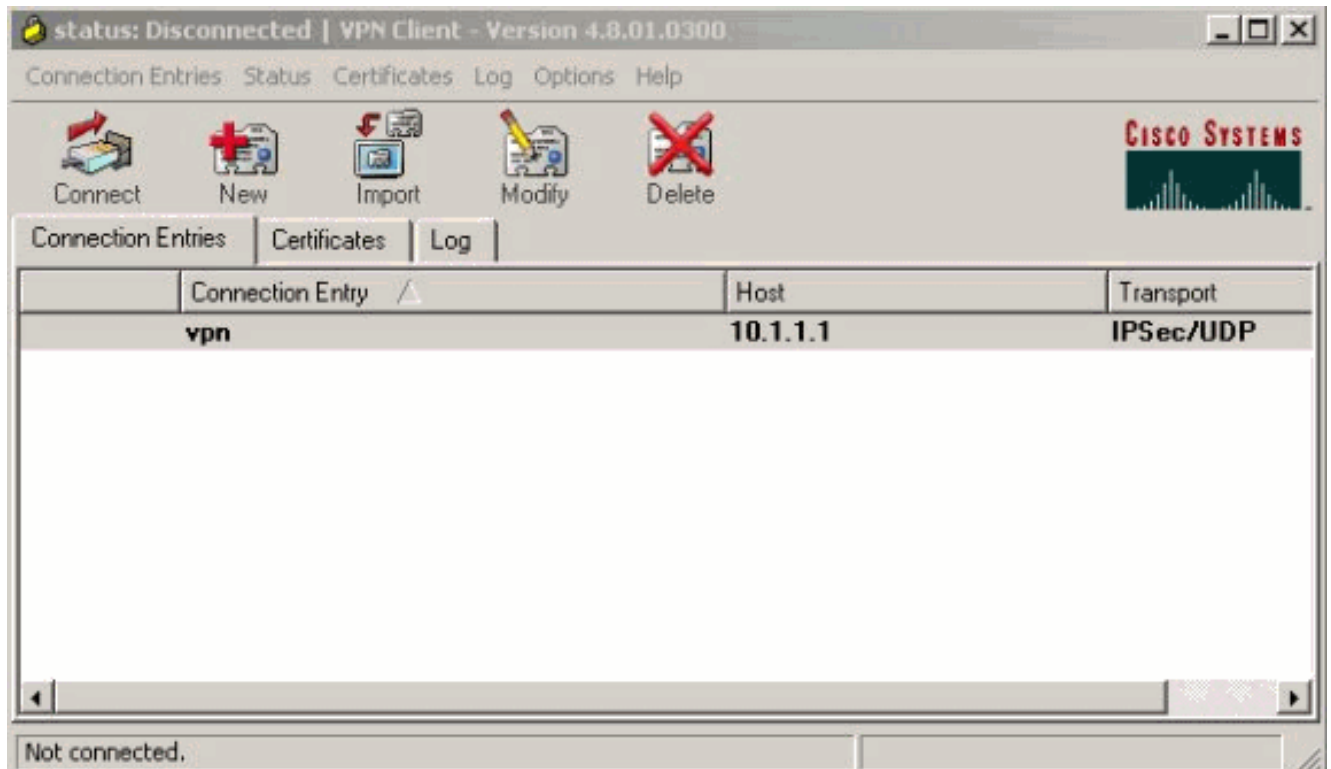
1. Escolha o **Iniciar > Programas > Cliente de VPN de Sistemas Cisco > o cliente VPN**.
2. Clique **novo** para lançar a janela de entrada nova da conexão de VPN da criação.



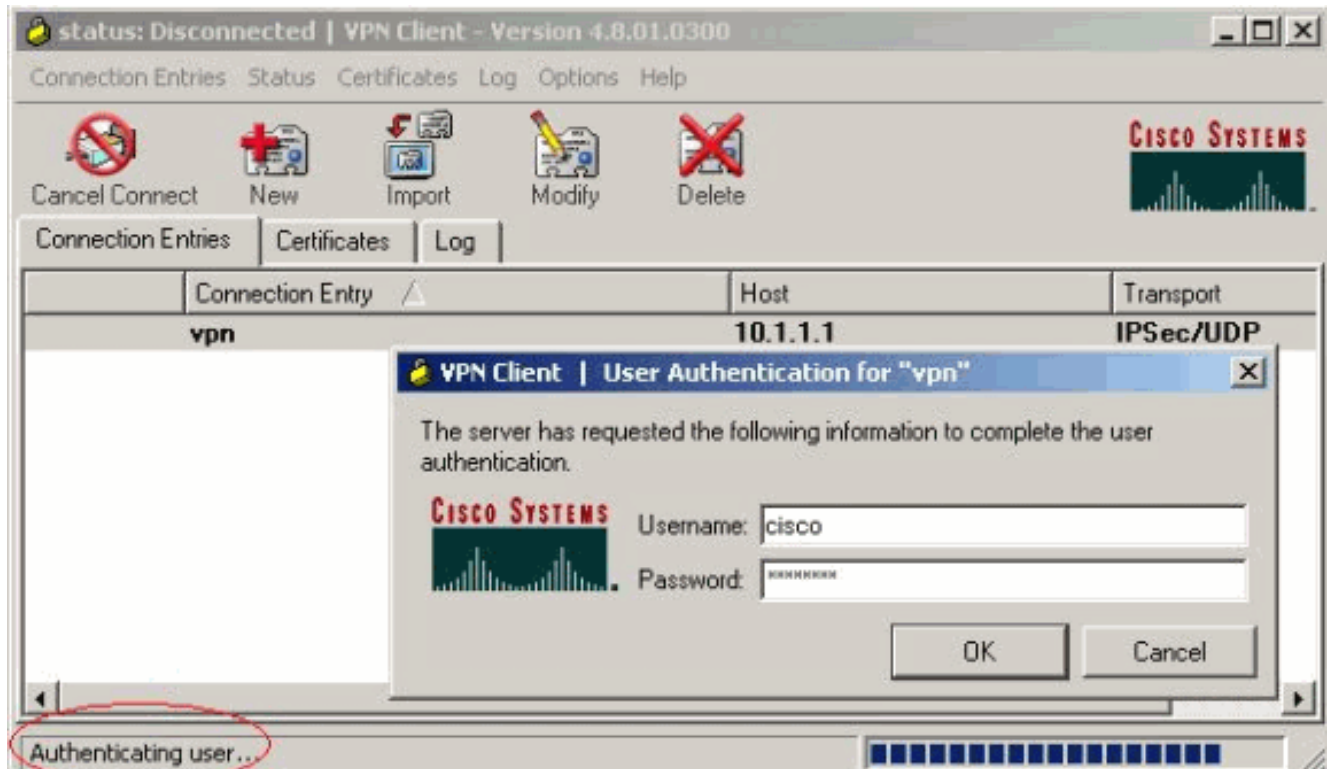
3. Dê entrada com o nome da entrada de conexão junto com uma descrição. Incorpore o endereço IP externo do roteador à caixa do host. Então, incorpore o nome do grupo VPN e a senha e clique a **salv guarda**.



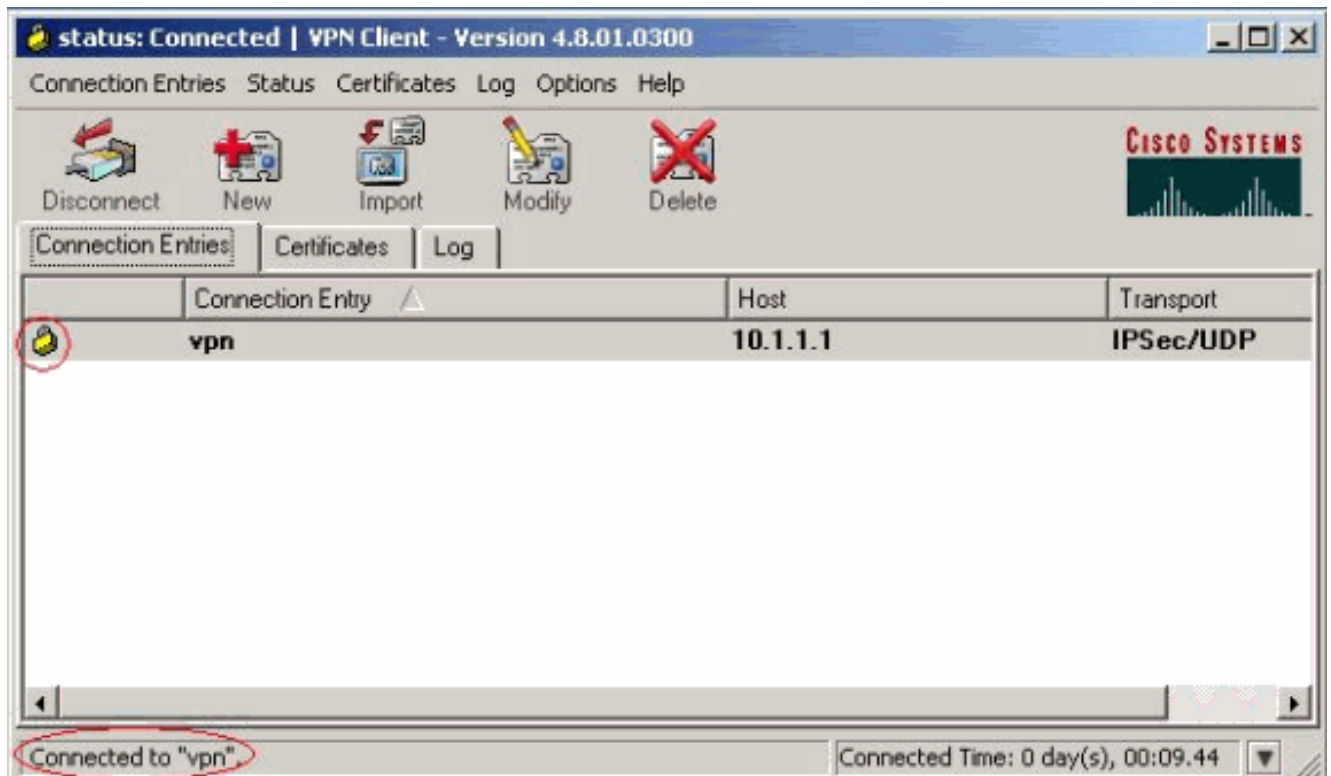
4. Clique sobre a conexão que você quer se usar e o clique **conecta** da janela principal do cliente VPN.



5. Quando alertado, incorpore a informação do nome de usuário e senha para o Xauth e clique a **APROVAÇÃO** para conectar à rede remota.



O cliente VPN obtém conectado com o roteador na instalação central.



## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

```
vpn2611#show crypto isakmp sa
```

```
dst          src          state          conn-id  slot
10.1.1.1    10.0.0.1    QM_IDLE          3        0
```

```
vpn2611#show crypto ipsec sa interface: Ethernet0/0
```

```
  Crypto map tag: clientmap, local addr. 10.1.1.1
```

```
local ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0)
```

```
remote ident (addr/mask/prot/port): (10.16.20.2/255.255.255.255/0/0)
```

```
current_peer: 10.0.0.1
```

```
  PERMIT, flags={}
```

```
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
```

```
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.0.0.1
```

```
path mtu 1500, media mtu 1500
```

```
current outbound spi: 77AFCCFA
```

```
inbound esp sas:
```

```
spi: 0xC7AC22AB(3349947051)
```

```
  transform: esp-3des esp-sha-hmac ,
```

```
  in use settings = {Tunnel, }
```

```
  slot: 0, conn id: 2000, flow_id: 1, crypto map: clientmap
```

```
  sa timing: remaining key lifetime (k/sec): (4608000/3444)
```

```
  IV size: 8 bytes
```

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x77AFCCFA(2008009978)  
transform: esp-3des esp-sha-hmac ,  
in use settings = {Tunnel, }  
slot: 0, conn id: 2001, flow\_id: 2, crypto map: clientmap  
sa timing: remaining key lifetime (k/sec): (4608000/3444)  
IV size: 8 bytes  
replay detection support: Y

outbound ah sas:

outbound pcp sas:

local ident (addr/mask/prot/port): (172.18.124.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.16.20.2/255.255.255.255/0/0)

**current\_peer: 10.0.0.1**

PERMIT, flags={}

**#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4**

**#pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6**

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.0.0.1

path mtu 1500, media mtu 1500

current outbound spi: 2EE5BF09

inbound esp sas:

spi: 0x3565451F(895829279)  
transform: esp-3des esp-sha-hmac ,  
in use settings = {Tunnel, }  
slot: 0, conn id: 2002, flow\_id: 3, crypto map: clientmap  
sa timing: remaining key lifetime (k/sec): (4607999/3469)  
IV size: 8 bytes  
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x2EE5BF09(786808585)  
transform: esp-3des esp-sha-hmac ,  
in use settings = {Tunnel, }  
slot: 0, conn id: 2003, flow\_id: 4, crypto map: clientmap  
sa timing: remaining key lifetime (k/sec): (4607999/3469)  
IV size: 8 bytes  
replay detection support: Y

outbound ah sas:

outbound pcp sas:

vpn2611#show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
3	Ethernet0/0	10.1.1.1	set	HMAC_SHA+3DES_56_C	0	0

2000	Ethernet0/0	10.1.1.1	set	HMAC_SHA+3DES_56_C	0	5
2001	Ethernet0/0	10.1.1.1	set	HMAC_SHA+3DES_56_C	5	0
2002	Ethernet0/0	10.1.1.1	set	HMAC_SHA+3DES_56_C	0	6
2003	Ethernet0/0	10.1.1.1	set	HMAC_SHA+3DES_56_C	4	0

## Troubleshooting

Use esta seção para resolver problemas de configuração.

### Comandos para Troubleshooting

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

**Nota:** Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos debug.

- **debug crypto ipsec** — Exibe informações de depuração sobre conexões de IPSec.
- **debug crypto isakmp** — Exibe informações de depuração sobre conexões de IPSec e mostra o primeiro conjunto de atributos negados devido a incompatibilidades em ambas as extremidades.
- **debug crypto engine** — Exibe informações a partir do cripto mecanismo.
- **debug aaa authentication** — Exibe informações sobre autenticação AAA/TACACS+.
- **debug aaa authorization radius** — Indica a informação na autorização AAA/TACACS+.
- **debugar o raio** — Informação dos indicadores em uma comunicação do Troubleshooting entre o servidor Radius e o roteador.

### Saída de depurações

Esta seção fornece informações de depuração do roteador, que podem ser usadas para resolver problemas na configuração.

### Registros de Roteador

```
vpn2611#show debug
```

```
General OS:
```

```
AAA Authorization debugging is on
```

```
Radius protocol debugging is on
```

```
Radius packet protocol debugging is on
```

```
Cryptographic Subsystem:
```

```
Crypto ISAKMP debugging is on
```

```
Crypto IPSEC debugging is on
```

```
vpn2611#
```

```
1w0d: ISAKMP (0:0): received packet from 10.0.0.1 (N) NEW SA
```

```
1w0d: ISAKMP: local port 500, remote port 500
```

```
1w0d: ISAKMP (0:2): (Re)Setting client xauth list userauthen and state
```

```
1w0d: ISAKMP: Locking CONFIG struct 0x830BF118 from
```

```
crypto_ikmp_config_initialize_sa, count 2
```

```
1w0d: ISAKMP (0:2): processing SA payload. message ID = 0
```

```
1w0d: ISAKMP (0:2): processing ID payload. message ID = 0
```

```
1w0d: ISAKMP (0:2): processing vendor id payload
```

```
1w0d: ISAKMP (0:2): vendor ID seems Unity/DPD but bad major
```

```
1w0d: ISAKMP (0:2): vendor ID is XAUTH
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): vendor ID is DPD
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): vendor ID is Unity
1w0d: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 3 policy
1w0d: ISAKMP: encryption 3DES-CBC
1w0d: ISAKMP: hash SHA
1w0d: ISAKMP: default group 2
1w0d: ISAKMP: auth XAUTHInitPreShared
1w0d: ISAKMP: life type in seconds
1w0d: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: ISAKMP (0:2): atts are acceptable. Next payload is 3
1w0d: ISAKMP (0:2): processing KE payload. message ID = 0
1w0d: ISAKMP (0:2): processing NONCE payload. message ID = 0
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1
1w0d: AAA/MEMORY: create_user (0x830CAF28) user='3000client' ruser='NULL'
ds0=0 port='ISAKMP-ID-AUTH' rem_addr='10.0.0.1' authen_type=NONE
service=LOGIN priv=0 initial_task_id='0'
1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT

1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552):
Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET
1w0d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(66832552) user='3000client'
1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): send AV service=ike
1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): send AV
protocol=ipsec
1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): found list
"groupauthor"
1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): Method=radius
(radius)
1w0d: RADIUS: authenticating to get author data
1w0d: RADIUS: ustruct sharecount=3
1w0d: Radius: radius_port_info() success=0 radius_nas_port=1
1w0d: RADIUS: Send to ISAKMP-ID-AUTH id 60 172.18.124.96:1645,
Access-Request, len 83
1w0d: RADIUS: authenticator AF EC D3 AD D6 39 4F 7D - A0 5E FC 64 F5 DE
A7 3B
1w0d: RADIUS: NAS-IP-Address [4] 6 172.18.124.159
1w0d: RADIUS: NAS-Port-Type [61] 6 Async [0]
1w0d: RADIUS: User-Name [1] 12 "3000client"
1w0d: RADIUS: Calling-Station-Id [31] 15 "10.0.0.1"
1w0d: RADIUS: User-Password [2] 18 *
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]
1w0d: RADIUS: Received from id 60 172.18.124.96:1645, Access-Accept, len
176
1w0d: RADIUS: authenticator 52 BA 0A 38 AC C2 2B 6F - A0 77 64 93 D6 19
78 CF
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]
1w0d: RADIUS: Vendor, Cisco [26] 30
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:key-exchange=ike"
1w0d: RADIUS: Vendor, Cisco [26] 40
1w0d: RADIUS: Cisco AVpair [1] 34 "ipsec:key-exchange=preshared-key"
1w0d: RADIUS: Vendor, Cisco [26] 30
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:addr-pool=ippool"
1w0d: RADIUS: Vendor, Cisco [26] 23
1w0d: RADIUS: Cisco AVpair [1] 17 "ipsec:inacl=108"
1w0d: RADIUS: Tunnel-Type [64] 6 01:ESP [9]
1w0d: RADIUS: Tunnel-Password [69] 21 *
1w0d: RADIUS: saved authorization data for user 830CAF28 at 83198648
```

```
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=ike"
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=preshared-key"
1w0d: RADIUS: cisco AVPair "ipsec:addr-pool=ippool"
1w0d: RADIUS: cisco AVPair "ipsec:inac1=108"
1w0d: RADIUS: Tunnel-Type, [01] 00 00 09
1w0d: RADIUS: TAS(1) created and enqueued.
1w0d: RADIUS: Tunnel-Password decrypted, [01] cisco123
1w0d: RADIUS: TAS(1) takes precedence over tagged attributes,
tunnel_type=esp
1w0d: RADIUS: free TAS(1)
1w0d: AAA/AUTHOR (66832552): Post authorization status = PASS_REPL
1w0d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV key-exchange=preshared-key
AAA/AUTHOR/IKE: Processing AV addr-pool=ippool
AAA/AUTHOR/IKE: Processing AV inac1=108
AAA/AUTHOR/IKE: Processing AV tunnel-type*esp
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV tunnel-tag*1
1w0d: ISAKMP (0:2): SKEYID state generated
1w0d: ISAKMP (0:2): SA is doing pre-shared key authentication plus XAUTH
using id type ID_IPV4_ADDR
1w0d: ISAKMP (2): ID payload
next-payload : 10
type : 1
protocol : 17
port : 500
length : 8
1w0d: ISAKMP (2): Total payload length: 12
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) AG_INIT_EXCH
1w0d: ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, PRESHARED_KEY_REPLY
Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

1w0d: AAA/MEMORY: free_user (0x830CAF28) user='3000client' ruser='NULL'
port='ISAKMP-ID-AUTH' rem_addr='10.0.0.1' authen_type=NONE
service=LOGIN priv=0
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) AG_INIT_EXCH
1w0d: ISAKMP (0:2): processing HASH payload. message ID = 0
1w0d: ISAKMP (0:2): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 831938B0
1w0d: ISAKMP (0:2): Process initial contact, bring down existing phase 1
and 2 SA's
1w0d: ISAKMP (0:2): returning IP addr to the address pool: 10.16.20.1
1w0d: ISAKMP (0:2): returning address 10.16.20.1 to pool
1w0d: ISAKMP (0:2): peer does not do paranoid keepalives.

1w0d: ISAKMP (0:2): SA has been authenticated with 10.0.0.1
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): purging node -1377537628
1w0d: ISAKMP: Sending phase 1 responder lifetime 86400

1w0d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

1w0d: IPSEC(key_engine): got a queue event...
1w0d: IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
1w0d: IPSEC(key_engine_delete_sas): delete all SAs shared with
10.0.0.1
1w0d: ISAKMP (0:2): Need XAUTH
1w0d: AAA: parse name=ISAKMP idb type=-1 tty=-1
1w0d: AAA/MEMORY: create_user (0x830CAF28) user='NULL' ruser='NULL' ds0=0
port='ISAKMP' rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN
priv=0 initial_task_id='0'
1w0d: ISAKMP (0:2): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
```



Old State = IKE\_P1\_COMPLETE New State = IKE\_XAUTH\_AAA\_START\_LOGIN\_AWAIT

1w0d: ISAKMP: got callback 1  
1w0d: ISAKMP/xauth: request attribute XAUTH\_TYPE\_V2  
1w0d: ISAKMP/xauth: request attribute XAUTH\_MESSAGE\_V2  
1w0d: ISAKMP/xauth: request attribute XAUTH\_USER\_NAME\_V2  
1w0d: ISAKMP/xauth: request attribute XAUTH\_USER\_PASSWORD\_V2  
1w0d: ISAKMP (0:2): initiating peer config to 10.0.0.1. ID =  
-1021889193  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) CONF\_XAUTH  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_AAA, IKE\_AAA\_START\_LOGIN  
Old State = IKE\_XAUTH\_AAA\_START\_LOGIN\_AWAIT New State =  
IKE\_XAUTH\_REQ\_SENT

1w0d: ISAKMP (0:1): purging node 832238598  
1w0d: ISAKMP (0:1): purging node 1913225491  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) CONF\_XAUTH  
1w0d: ISAKMP (0:2): processing transaction payload from 10.0.0.1.  
message ID = -1021889193  
1w0d: ISAKMP: Config payload REPLY  
1w0d: ISAKMP/xauth: reply attribute XAUTH\_TYPE\_V2 unexpected  
1w0d: ISAKMP/xauth: reply attribute XAUTH\_USER\_NAME\_V2  
1w0d: ISAKMP/xauth: reply attribute XAUTH\_USER\_PASSWORD\_V2  
1w0d: ISAKMP (0:2): deleting node -1021889193 error FALSE reason "done  
with xauth request/reply exchange"  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_PEER, IKE\_CFG\_REPLY  
Old State = IKE\_XAUTH\_REQ\_SENT New State = IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT

1w0d: RADIUS: ustruct sharecount=2  
1w0d: Radius: radius\_port\_info() success=0 radius\_nas\_port=1  
**1w0d: RADIUS: Send to ISAKMP id 61 172.18.124.96:1645, Access-Request, len 72**  
1w0d: RADIUS: authenticator 98 12 4F C0 DA B9 48 B8 - 58 00 BA 14 08 8E  
87 C0  
1w0d: RADIUS: NAS-IP-Address [4] 6 172.18.124.159  
1w0d: RADIUS: NAS-Port-Type [61] 6 Async [0]  
**1w0d: RADIUS: User-Name [1] 7 "cisco"**  
1w0d: RADIUS: Calling-Station-Id [31] 15 "10.0.0.1"  
1w0d: RADIUS: User-Password [2] 18 \*  
**1w0d: RADIUS: Received from id 61 172.18.124.96:1645, Access-Accept, len 26**  
1w0d: RADIUS: authenticator 00 03 F4 E1 9C 61 3F 03 - 54 83 E8 27 5C 6A  
7B 6E  
1w0d: RADIUS: Framed-IP-Address [8] 6 255.255.255.255  
1w0d: RADIUS: saved authorization data for user 830CAF28 at 830F89F8  
1w0d: ISAKMP: got callback 1  
1w0d: ISAKMP (0:2): initiating peer config to 10.0.0.1. ID =  
-547189328  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) CONF\_XAUTH  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_AAA, IKE\_AAA\_CONT\_LOGIN  
Old State = IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT New State = IKE\_XAUTH\_SET\_SENT

1w0d: AAA/MEMORY: free\_user (0x830CAF28) user='cisco' ruser='NULL'  
port='ISAKMP' rem\_addr='10.0.0.1' authen\_type=ASCII service=LOGIN  
priv=0  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) CONF\_XAUTH  
1w0d: ISAKMP (0:2): processing transaction payload from 10.0.0.1.  
message ID = -547189328  
1w0d: ISAKMP: Config payload ACK  
1w0d: ISAKMP (0:2): XAUTH ACK Processed  
1w0d: ISAKMP (0:2): deleting node -547189328 error FALSE reason "done with  
transaction"  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_PEER, IKE\_CFG\_ACK  
Old State = IKE\_XAUTH\_SET\_SENT New State = IKE\_P1\_COMPLETE  
  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_INTERNAL, IKE\_PHASE1\_COMPLETE

Old State = IKE\_P1\_COMPLETE New State = IKE\_P1\_COMPLETE

1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM\_IDLE  
1w0d: ISAKMP (0:2): processing transaction payload from 10.0.0.1.  
message ID = -1911189201  
1w0d: ISAKMP: Config payload REQUEST  
1w0d: ISAKMP (0:2): checking request:  
1w0d: ISAKMP: IP4\_ADDRESS  
1w0d: ISAKMP: IP4\_NETMASK  
1w0d: ISAKMP: IP4\_DNS  
1w0d: ISAKMP: IP4\_NBNS  
1w0d: ISAKMP: ADDRESS\_EXPIRY  
1w0d: ISAKMP: APPLICATION\_VERSION  
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7000  
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7001  
1w0d: ISAKMP: DEFAULT\_DOMAIN  
1w0d: ISAKMP: SPLIT\_INCLUDE  
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7007  
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7008  
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7005  
1w0d: AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1  
1w0d: AAA/MEMORY: create\_user (0x830CAF28) user='3000client' ruser='NULL'  
ds0=0 port='ISAKMP-GROUP-AUTH' rem\_addr='10.0.0.1' authen\_type=NONE  
service=LOGIN priv=0 initial\_task\_id='0'  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_PEER, IKE\_CFG\_REQUEST  
Old State = IKE\_P1\_COMPLETE New State = IKE\_CONFIG\_AUTHOR\_AAA\_AWAIT

1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746):  
Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET  
1w0d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(3098118746)  
user='3000client'  
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): send AV  
service=ike  
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): send AV  
protocol=ipsec  
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): found list  
"groupauthor"  
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): Method=radius  
(radius)  
1w0d: RADIUS: authenticating to get author data  
1w0d: RADIUS: ustruct sharecount=3  
1w0d: Radius: radius\_port\_info() success=0 radius\_nas\_port=1  
1w0d: RADIUS: Send to ISAKMP-GROUP-AUTH id 62 172.18.124.96:1645,  
Access-Request, len 83  
1w0d: RADIUS: authenticator 32 C5 32 FF AB B7 E4 68 - 9A 68 5A DE D5 56  
0C BE  
1w0d: RADIUS: NAS-IP-Address [4] 6 172.18.124.159  
1w0d: RADIUS: NAS-Port-Type [61] 6 Async [0]  
1w0d: RADIUS: User-Name [1] 12 "3000client"  
1w0d: RADIUS: Calling-Station-Id [31] 15 "10.0.0.1"  
1w0d: RADIUS: User-Password [2] 18 \*  
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]  
1w0d: RADIUS: Received from id 62 172.18.124.96:1645, Access-Accept, len  
176  
1w0d: RADIUS: authenticator DF FA FE 21 07 92 4F 10 - 75 5E D6 96 66 70  
19 27  
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]  
1w0d: RADIUS: Vendor, Cisco [26] 30  
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:key-exchange=ike"  
1w0d: RADIUS: Vendor, Cisco [26] 40  
1w0d: RADIUS: Cisco AVpair [1] 34  
"ipsec:key-exchange=preshared-key"  
1w0d: RADIUS: Vendor, Cisco [26] 30  
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:addr-pool=ippool"

```
1w0d: RADIUS: Vendor, Cisco [26] 23
1w0d: RADIUS: Cisco AVpair [1] 17 "ipsec:inacl=108"
1w0d: RADIUS: Tunnel-Type [64] 6 01:ESP [9]
1w0d: RADIUS: Tunnel-Password [69] 21 *
1w0d: RADIUS: saved authorization data for user 830CAF28 at 83143E64
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=ike"
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=preshared-key"
1w0d: RADIUS: cisco AVPair "ipsec:addr-pool=ippool"
1w0d: RADIUS: cisco AVPair "ipsec:inacl=108"
1w0d: RADIUS: Tunnel-Type, [01] 00 00 09
1w0d: RADIUS: TAS(1) created and enqueued.
1w0d: RADIUS: Tunnel-Password decrypted, [01] cisco123
1w0d: RADIUS: TAS(1) takes precedence over tagged attributes,
tunnel_type=esp
1w0d: RADIUS: free TAS(1)
1w0d: AAA/AUTHOR (3098118746): Post authorization status = PASS_REPL
1w0d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV key-exchange=preshared-key
AAA/AUTHOR/IKE: Processing AV addr-pool=ippool
AAA/AUTHOR/IKE: Processing AV inacl=108
AAA/AUTHOR/IKE: Processing AV tunnel-type*esp
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV tunnel-tag*1
1w0d: ISAKMP (0:2): attributes sent in message:
1w0d: Address: 0.2.0.0
1w0d: ISAKMP (0:2): allocating address 10.16.20.2
1w0d: ISAKMP: Sending private address: 10.16.20.2
1w0d: ISAKMP: Unknown Attr: IP4_NETMASK (0x2)
1w0d: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address:
86395
1w0d: ISAKMP: Sending APPLICATION_VERSION string: Cisco Internetwork
Operating System Software
IOS (tm) C2600 Software (C2600-JK903S-M), Version 12.2(8)T, RELEASE
SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 14-Feb-02 16:50 by ccai
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7000)
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7001)
1w0d: ISAKMP: Sending split include name 108 network 14.38.0.0 mask
255.255.0.0 protocol 0, src port 0, dst port 0

1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7007)
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7008)
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7005)
1w0d: ISAKMP (0:2): responding to peer config from 10.0.0.1. ID =
-1911189201
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) CONF_ADDR
1w0d: ISAKMP (0:2): deleting node -1911189201 error FALSE reason ""
1w0d: ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR
Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

1w0d: AAA/MEMORY: free_user (0x830CAF28) user='3000client' ruser='NULL'
port='ISAKMP-GROUP-AUTH' rem_addr='10.0.0.1' authen_type=NONE
service=LOGIN priv=0
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): processing HASH payload. message ID = 132557281
1w0d: ISAKMP (0:2): processing SA payload. message ID = 132557281
1w0d: ISAKMP (0:2): Checking IPsec proposal 1
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-MD5
1w0d: ISAKMP: encaps is 1
```

1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 1) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): skipping next ANDED proposal (1)  
1w0d: ISAKMP (0:2): Checking IPsec proposal 2  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-SHA  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: ISAKMP (0:2): atts are acceptable.  
1w0d: ISAKMP (0:2): Checking IPsec proposal 2  
1w0d: ISAKMP (0:2): transform 1, IPPCP LZS  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 4, trans 3, hmac\_alg 0) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): Checking IPsec proposal 3  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-MD5  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 1) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): Checking IPsec proposal 4  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-SHA  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
**1w0d: ISAKMP (0:2): atts are acceptable.**  
1w0d: IPSEC(validate\_proposal\_request): proposal part #1,  
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,  
local\_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1),  
remote\_proxy= 10.16.20.2/255.255.255.255/0/0 (type=1),  
protocol= ESP, transform= esp-3des esp-sha-hmac ,  
lifedur= 0s and 0kb,  
spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4  
1w0d: ISAKMP (0:2): processing NONCE payload. message ID = 132557281  
1w0d: ISAKMP (0:2): processing ID payload. message ID = 132557281  
1w0d: ISAKMP (0:2): processing ID payload. message ID = 132557281  
1w0d: ISAKMP (0:2): asking for 1 spis from ipsec  
1w0d: ISAKMP (0:2): Node 132557281, Input = IKE\_MSG\_FROM\_PEER,  
IKE\_QM\_EXCH  
Old State = IKE\_QM\_READY New State = IKE\_QM\_SPI\_STARVE  
  
1w0d: IPSEC(key\_engine): got a queue event...  
1w0d: IPSEC(spi\_response): getting spi 245824456 for SA  
from 10.1.1.1 to 10.0.0.1 for prot 3  
1w0d: ISAKMP: received ke message (2/1)  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM\_IDLE  
1w0d: ISAKMP (0:2): Node 132557281, Input = IKE\_MSG\_FROM\_IPSEC,  
IKE\_SPI\_REPLY  
Old State = IKE\_QM\_SPI\_STARVE New State = IKE\_QM\_R\_QM2

1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM\_IDLE  
1w0d: ISAKMP (0:2): Creating IPsec SAs  
1w0d: inbound SA from 10.0.0.1 to 10.1.1.1  
(proxy 10.16.20.2 to 10.1.1.1)  
1w0d: has spi 0xEA6FBC8 and conn\_id 2000 and flags 4  
1w0d: lifetime of 2147483 seconds  
1w0d: outbound SA from 10.1.1.1 to 10.0.0.1 (proxy  
10.1.1.1 to 10.16.20.2 )  
1w0d: has spi 1009463339 and conn\_id 2001 and flags C  
1w0d: lifetime of 2147483 seconds  
1w0d: ISAKMP (0:2): deleting node 132557281 error FALSE reason "quick mode  
done (await())"  
1w0d: ISAKMP (0:2): Node 132557281, Input = IKE\_MSG\_FROM\_PEER,  
IKE\_QM\_EXCH  
Old State = IKE\_QM\_R\_QM2 New State = IKE\_QM\_PHASE2\_COMPLETE

1w0d: IPSEC(key\_engine): got a queue event...  
1w0d: IPSEC(initialize\_sas): ,  
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,  
local\_proxy= 10.1.1.1/0.0.0.0/0/0 (type=1),  
remote\_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),  
protocol= ESP, transform= esp-3des esp-sha-hmac ,  
lifedur= 2147483s and 0kb,  
spi= 0xEA6FBC8(245824456), conn\_id= 2000, keysize= 0, flags= 0x4  
1w0d: IPSEC(initialize\_sas): ,  
(key eng. msg.) OUTBOUND local= 10.1.1.1, remote= 10.0.0.1,  
local\_proxy= 10.1.1.1/0.0.0.0/0/0 (type=1),  
remote\_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),  
protocol= ESP, transform= esp-3des esp-sha-hmac ,  
lifedur= 2147483s and 0kb,  
spi= 0x3C2B302B(1009463339), conn\_id= 2001, keysize= 0, flags= 0xC  
1w0d: IPSEC(create\_sa): sa created,  
(sa) sa\_dest= 10.1.1.1, sa\_prot= 50,  
sa\_spi= 0xEA6FBC8(245824456),  
sa\_trans= esp-3des esp-sha-hmac , sa\_conn\_id= 2000  
1w0d: IPSEC(create\_sa): sa created,  
(sa) sa\_dest= 10.0.0.1, sa\_prot= 50,  
sa\_spi= 0x3C2B302B(1009463339),  
sa\_trans= esp-3des esp-sha-hmac , sa\_conn\_id= 2001  
1w0d: ISAKMP: received ke message (4/1)  
1w0d: ISAKMP: Locking CONFIG struct 0x830BF118 for  
crypto\_ikmp\_config\_handle\_kei\_mess, count 3  
1w0d: ISAKMP (0:1): purging SA., sa=83196748, delme=83196748  
1w0d: ISAKMP: Unlocking CONFIG struct 0x830BF118 on return of attributes,  
count 2  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM\_IDLE  
1w0d: ISAKMP (0:2): processing HASH payload. message ID = -1273332908  
1w0d: ISAKMP (0:2): processing SA payload. message ID = -1273332908  
1w0d: ISAKMP (0:2): Checking IPsec proposal 1  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-MD5  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 3, trans 3,  
hmac\_alg 1) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): skipping next ANDed proposal (1)  
1w0d: ISAKMP (0:2): Checking IPsec proposal 2  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-SHA

lw0d: ISAKMP: encaps is 1  
lw0d: ISAKMP: SA life type in seconds  
lw0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
lw0d: ISAKMP (0:2): atts are acceptable.  
lw0d: ISAKMP (0:2): Checking IPsec proposal 2  
lw0d: ISAKMP (0:2): transform 1, IPPCP LZS  
lw0d: ISAKMP: attributes in transform:  
lw0d: ISAKMP: encaps is 1  
lw0d: ISAKMP: SA life type in seconds  
lw0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
lw0d: IPSEC(validate\_proposal): transform proposal (prot 4, trans 3, hmac\_alg 0) not supported  
lw0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
lw0d: ISAKMP (0:2): Checking IPsec proposal 3  
lw0d: ISAKMP: transform 1, ESP\_3DES  
lw0d: ISAKMP: attributes in transform:  
lw0d: ISAKMP: authenticator is HMAC-MD5  
lw0d: ISAKMP: encaps is 1  
lw0d: ISAKMP: SA life type in seconds  
lw0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
lw0d: IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 1) not supported  
lw0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
lw0d: ISAKMP (0:2): Checking IPsec proposal 4  
lw0d: ISAKMP: transform 1, ESP\_3DES  
lw0d: ISAKMP: attributes in transform:  
lw0d: ISAKMP: authenticator is HMAC-SHA  
lw0d: ISAKMP: encaps is 1  
lw0d: ISAKMP: SA life type in seconds  
lw0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
lw0d: ISAKMP (0:2): atts are acceptable.  
lw0d: IPSEC(validate\_proposal\_request): proposal part #  
vpn2611#1,  
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,  
local\_proxy= 14.38.0.0/255.255.0.0/0/0 (type=4),  
remote\_proxy= 10.16.20.2/255.255.255.255/0/0 (type=1),  
protocol= ESP, transform= esp-3des esp-sha-hmac ,  
lifedur= 0s and 0kb,  
spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4  
lw0d: ISAKMP (0:2): processing NONCE payload. message ID = -1273332908  
lw0d: ISAKMP (0:2): processing ID payload. message ID = -1273332908  
lw0d: ISAKMP (0:2): processing ID payload. message ID = -1273332908  
lw0d: ISAKMP (0:2): asking for 1 spis from ipsec  
lw0d: ISAKMP (0:2): Node -1273332908, Input = IKE\_MSG\_FROM\_PEER,  
IKE\_QM\_EXCH  
Old State = IKE\_QM\_READY New State = IKE\_QM\_SPI\_STARVE  
  
lw0d: IPSEC(key\_engine): got a queue event...  
lw0d: IPSEC(spi\_response): getting spi 593097454 for SA  
from 10.1.1.1 to 10.0.0.1  
vpn2611#  
vpn2611#2 for prot 3  
lw0d: ISAKMP: received ke message (2/1)  
lw0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM\_IDLE  
lw0d: ISAKMP (0:2): Node -1273332908, Input = IKE\_MSG\_FROM\_IPSEC,  
IKE\_SPI\_REPLY  
Old State = IKE\_QM\_SPI\_STARVE New State = IKE\_QM\_R\_QM2  
  
lw0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM\_IDLE  
**lw0d: ISAKMP (0:2): Creating IPsec SAs**  
**lw0d: inbound SA from 10.0.0.1 to 10.1.1.1**  
**(proxy 10.16.20.2 to 14.38.0.0)**  
**lw0d: has spi 0x2359F2EE and conn\_id 2002 and flags 4**  
**lw0d: lifetime of 2147483 seconds**

```
1w0d: outbound SA from 10.1.1.1 to 10.0.0.1 (proxy
14.38.0.0 to 10.16.20.2 )
1w0d: has spi 1123818858 and conn_id 2003 and flags C
1w0d: lifetime of 2147483 seconds
1w0d: ISAKMP (0:2): deleting node -1273332908 erro
vpn2611#un ar FALSE reason "quick mode done (await())"
1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

1w0d: IPSEC(key_engine): got a queue event...
1w0d: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,
local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x2359F2EE(593097454), conn_id= 2002, keysize= 0, flags= 0x4
1w0d: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.1.1.1, remote= 10.0.0.1,
local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sh11
All possible debugging has been turned off
vpn2611#a-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x42FC1D6A(1123818858), conn_id= 2003, keysize= 0, flags= 0xC
1w0d: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.1.1, sa_prot= 50,
sa_spi= 0x2359F2EE(593097454),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2002
1w0d: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.0.0.1, sa_prot= 50,
sa_spi= 0x42FC1D6A(1123818858),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2003
```

## Registros de Cliente

Lance o LogViewer no cliente VPN a fim ver os logs. Certifique-se de que o filtro está ajustado à elevação para todas as classes configuradas. Este é um registro de saída da amostra:

```
vpn2611#show debug
General OS:
AAA Authorization debugging is on
Radius protocol debugging is on
Radius packet protocol debugging is on

Cryptographic Subsystem:
Crypto ISAKMP debugging is on
Crypto IPSEC debugging is on
vpn2611#

1w0d: ISAKMP (0:0): received packet from 10.0.0.1 (N) NEW SA
1w0d: ISAKMP: local port 500, remote port 500
1w0d: ISAKMP (0:2): (Re)Setting client xauth list userauthen and state
1w0d: ISAKMP: Locking CONFIG struct 0x830BF118 from
crypto_ikmp_config_initialize_sa, count 2
1w0d: ISAKMP (0:2): processing SA payload. message ID = 0
1w0d: ISAKMP (0:2): processing ID payload. message ID = 0
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): vendor ID seems Unity/DPD but bad major
1w0d: ISAKMP (0:2): vendor ID is XAUTH
1w0d: ISAKMP (0:2): processing vendor id payload
```

```
1w0d: ISAKMP (0:2): vendor ID is DPD
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): vendor ID is Unity
1w0d: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 3 policy
1w0d: ISAKMP: encryption 3DES-CBC
1w0d: ISAKMP: hash SHA
1w0d: ISAKMP: default group 2
1w0d: ISAKMP: auth XAUTHInitPreShared
1w0d: ISAKMP: life type in seconds
1w0d: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: ISAKMP (0:2): atts are acceptable. Next payload is 3
1w0d: ISAKMP (0:2): processing KE payload. message ID = 0
1w0d: ISAKMP (0:2): processing NONCE payload. message ID = 0
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1
1w0d: AAA/MEMORY: create_user (0x830CAF28) user='3000client' ruser='NULL'
ds0=0 port='ISAKMP-ID-AUTH' rem_addr='10.0.0.1' authen_type=NONE
service=LOGIN priv=0 initial_task_id='0'
1w0d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT

1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552):
Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET
1w0d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(66832552) user='3000client'
1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): send AV service=ike
1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): send AV
protocol=ipsec
1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): found list
"groupauthor"
1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): Method=radius
(radius)
1w0d: RADIUS: authenticating to get author data
1w0d: RADIUS: ustruct sharecount=3
1w0d: Radius: radius_port_info() success=0 radius_nas_port=1
1w0d: RADIUS: Send to ISAKMP-ID-AUTH id 60 172.18.124.96:1645,
Access-Request, len 83
1w0d: RADIUS: authenticator AF EC D3 AD D6 39 4F 7D - A0 5E FC 64 F5 DE
A7 3B
1w0d: RADIUS: NAS-IP-Address [4] 6 172.18.124.159
1w0d: RADIUS: NAS-Port-Type [61] 6 Async [0]
1w0d: RADIUS: User-Name [1] 12 "3000client"
1w0d: RADIUS: Calling-Station-Id [31] 15 "10.0.0.1"
1w0d: RADIUS: User-Password [2] 18 *
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]
1w0d: RADIUS: Received from id 60 172.18.124.96:1645, Access-Accept, len
176
1w0d: RADIUS: authenticator 52 BA 0A 38 AC C2 2B 6F - A0 77 64 93 D6 19
78 CF
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]
1w0d: RADIUS: Vendor, Cisco [26] 30
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:key-exchange=ike"
1w0d: RADIUS: Vendor, Cisco [26] 40
1w0d: RADIUS: Cisco AVpair [1] 34 "ipsec:key-exchange=preshared-key"
1w0d: RADIUS: Vendor, Cisco [26] 30
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:addr-pool=ippool"
1w0d: RADIUS: Vendor, Cisco [26] 23
1w0d: RADIUS: Cisco AVpair [1] 17 "ipsec:inacl=108"
1w0d: RADIUS: Tunnel-Type [64] 6 01:ESP [9]
1w0d: RADIUS: Tunnel-Password [69] 21 *
1w0d: RADIUS: saved authorization data for user 830CAF28 at 83198648
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=ike"
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=preshared-key"
```



```
1w0d: RADIUS: cisco AVPair "ipsec:addr-pool=ippool"
1w0d: RADIUS: cisco AVPair "ipsec:inac1=108"
1w0d: RADIUS: Tunnel-Type, [01] 00 00 09
1w0d: RADIUS: TAS(1) created and enqueued.
1w0d: RADIUS: Tunnel-Password decrypted, [01] cisco123
1w0d: RADIUS: TAS(1) takes precedence over tagged attributes,
tunnel_type=esp
1w0d: RADIUS: free TAS(1)
1w0d: AAA/AUTHOR (66832552): Post authorization status = PASS_REPL
1w0d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV key-exchange=preshared-key
AAA/AUTHOR/IKE: Processing AV addr-pool=ippool
AAA/AUTHOR/IKE: Processing AV inac1=108
AAA/AUTHOR/IKE: Processing AV tunnel-type*esp
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV tunnel-tag*1
1w0d: ISAKMP (0:2): SKEYID state generated
1w0d: ISAKMP (0:2): SA is doing pre-shared key authentication plus XAUTH
using id type ID_IPV4_ADDR
1w0d: ISAKMP (2): ID payload
next-payload : 10
type : 1
protocol : 17
port : 500
length : 8
1w0d: ISAKMP (2): Total payload length: 12
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) AG_INIT_EXCH
1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

1w0d: AAA/MEMORY: free_user (0x830CAF28) user='3000client' ruser='NULL'
port='ISAKMP-ID-AUTH' rem_addr='10.0.0.1' authen_type=NONE
service=LOGIN priv=0
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) AG_INIT_EXCH
1w0d: ISAKMP (0:2): processing HASH payload. message ID = 0
1w0d: ISAKMP (0:2): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 831938B0
1w0d: ISAKMP (0:2): Process initial contact, bring down existing phase 1
and 2 SA's
1w0d: ISAKMP (0:2): returning IP addr to the address pool: 10.16.20.1
1w0d: ISAKMP (0:2): returning address 10.16.20.1 to pool
1w0d: ISAKMP (0:2): peer does not do paranoid keepalives.

1w0d: ISAKMP (0:2): SA has been authenticated with 10.0.0.1
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): purging node -1377537628
1w0d: ISAKMP: Sending phase 1 responder lifetime 86400

1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

1w0d: IPSEC(key_engine): got a queue event...
1w0d: IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
1w0d: IPSEC(key_engine_delete_sas): delete all SAs shared with
10.0.0.1
1w0d: ISAKMP (0:2): Need XAUTH
1w0d: AAA: parse name=ISAKMP idb type=-1 tty=-1
1w0d: AAA/MEMORY: create_user (0x830CAF28) user='NULL' ruser='NULL' ds0=0
port='ISAKMP' rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN
priv=0 initial_task_id='0'
1w0d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
```

1w0d: ISAKMP: got callback 1  
1w0d: ISAKMP/xauth: request attribute XAUTH\_TYPE\_V2  
1w0d: ISAKMP/xauth: request attribute XAUTH\_MESSAGE\_V2  
1w0d: ISAKMP/xauth: request attribute XAUTH\_USER\_NAME\_V2  
1w0d: ISAKMP/xauth: request attribute XAUTH\_USER\_PASSWORD\_V2  
1w0d: ISAKMP (0:2): initiating peer config to 10.0.0.1. ID =  
-1021889193  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) CONF\_XAUTH  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_AAA, IKE\_AAA\_START\_LOGIN  
Old State = IKE\_XAUTH\_AAA\_START\_LOGIN\_AWAIT New State =  
IKE\_XAUTH\_REQ\_SENT  
  
1w0d: ISAKMP (0:1): purging node 832238598  
1w0d: ISAKMP (0:1): purging node 1913225491  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) CONF\_XAUTH  
1w0d: ISAKMP (0:2): processing transaction payload from 10.0.0.1.  
message ID = -1021889193  
1w0d: ISAKMP: Config payload REPLY  
1w0d: ISAKMP/xauth: reply attribute XAUTH\_TYPE\_V2 unexpected  
1w0d: ISAKMP/xauth: reply attribute XAUTH\_USER\_NAME\_V2  
1w0d: ISAKMP/xauth: reply attribute XAUTH\_USER\_PASSWORD\_V2  
1w0d: ISAKMP (0:2): deleting node -1021889193 error FALSE reason "done  
with xauth request/reply exchange"  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_PEER, IKE\_CFG\_REPLY  
Old State = IKE\_XAUTH\_REQ\_SENT New State = IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT  
  
1w0d: RADIUS: ustruct sharecount=2  
1w0d: Radius: radius\_port\_info() success=0 radius\_nas\_port=1  
**1w0d: RADIUS: Send to ISAKMP id 61 172.18.124.96:1645, Access-Request, len 72**  
1w0d: RADIUS: authenticator 98 12 4F C0 DA B9 48 B8 - 58 00 BA 14 08 8E  
87 C0  
1w0d: RADIUS: NAS-IP-Address [4] 6 172.18.124.159  
1w0d: RADIUS: NAS-Port-Type [61] 6 Async [0]  
**1w0d: RADIUS: User-Name [1] 7 "cisco"**  
1w0d: RADIUS: Calling-Station-Id [31] 15 "10.0.0.1"  
1w0d: RADIUS: User-Password [2] 18 \*  
**1w0d: RADIUS: Received from id 61 172.18.124.96:1645, Access-Accept, len 26**  
1w0d: RADIUS: authenticator 00 03 F4 E1 9C 61 3F 03 - 54 83 E8 27 5C 6A  
7B 6E  
1w0d: RADIUS: Framed-IP-Address [8] 6 255.255.255.255  
1w0d: RADIUS: saved authorization data for user 830CAF28 at 830F89F8  
1w0d: ISAKMP: got callback 1  
1w0d: ISAKMP (0:2): initiating peer config to 10.0.0.1. ID =  
-547189328  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) CONF\_XAUTH  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_AAA, IKE\_AAA\_CONT\_LOGIN  
Old State = IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT New State = IKE\_XAUTH\_SET\_SENT  
  
1w0d: AAA/MEMORY: free\_user (0x830CAF28) user='cisco' ruser='NULL'  
port='ISAKMP' rem\_addr='10.0.0.1' authen\_type=ASCII service=LOGIN  
priv=0  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) CONF\_XAUTH  
1w0d: ISAKMP (0:2): processing transaction payload from 10.0.0.1.  
message ID = -547189328  
1w0d: ISAKMP: Config payload ACK  
1w0d: ISAKMP (0:2): XAUTH ACK Processed  
1w0d: ISAKMP (0:2): deleting node -547189328 error FALSE reason "done with  
transaction"  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_PEER, IKE\_CFG\_ACK  
Old State = IKE\_XAUTH\_SET\_SENT New State = IKE\_P1\_COMPLETE  
  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_INTERNAL, IKE\_PHASE1\_COMPLETE  
Old State = IKE\_P1\_COMPLETE New State = IKE\_P1\_COMPLETE

```
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): processing transaction payload from 10.0.0.1.
message ID = -1911189201
1w0d: ISAKMP: Config payload REQUEST
1w0d: ISAKMP (0:2): checking request:
1w0d: ISAKMP: IP4_ADDRESS
1w0d: ISAKMP: IP4_NETMASK
1w0d: ISAKMP: IP4_DNS
1w0d: ISAKMP: IP4_NBNS
1w0d: ISAKMP: ADDRESS_EXPIRY
1w0d: ISAKMP: APPLICATION_VERSION
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7000
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7001
1w0d: ISAKMP: DEFAULT_DOMAIN
1w0d: ISAKMP: SPLIT_INCLUDE
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7007
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7008
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7005
1w0d: AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1
1w0d: AAA/MEMORY: create_user (0x830CAF28) user='3000client' ruser='NULL'
ds0=0 port='ISAKMP-GROUP-AUTH' rem_addr='10.0.0.1' authen_type=NONE
service=LOGIN priv=0 initial_task_id='0'
1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746):
Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET
1w0d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(3098118746)
user='3000client'
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): send AV
service=ike
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): send AV
protocol=ipsec
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): found list
"groupauthor"
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): Method=radius
(radius)
1w0d: RADIUS: authenticating to get author data
1w0d: RADIUS: ustruct sharecount=3
1w0d: Radius: radius_port_info() success=0 radius_nas_port=1
1w0d: RADIUS: Send to ISAKMP-GROUP-AUTH id 62 172.18.124.96:1645,
Access-Request, len 83
1w0d: RADIUS: authenticator 32 C5 32 FF AB B7 E4 68 - 9A 68 5A DE D5 56
0C BE
1w0d: RADIUS: NAS-IP-Address [4] 6 172.18.124.159
1w0d: RADIUS: NAS-Port-Type [61] 6 Async [0]
1w0d: RADIUS: User-Name [1] 12 "3000client"
1w0d: RADIUS: Calling-Station-Id [31] 15 "10.0.0.1"
1w0d: RADIUS: User-Password [2] 18 *
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]
1w0d: RADIUS: Received from id 62 172.18.124.96:1645, Access-Accept, len
176
1w0d: RADIUS: authenticator DF FA FE 21 07 92 4F 10 - 75 5E D6 96 66 70
19 27
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]
1w0d: RADIUS: Vendor, Cisco [26] 30
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:key-exchange=ike"
1w0d: RADIUS: Vendor, Cisco [26] 40
1w0d: RADIUS: Cisco AVpair [1] 34
"ipsec:key-exchange=preshared-key"
1w0d: RADIUS: Vendor, Cisco [26] 30
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:addr-pool=ippool"
1w0d: RADIUS: Vendor, Cisco [26] 23
1w0d: RADIUS: Cisco AVpair [1] 17 "ipsec:inacl=108"
```

```
1w0d: RADIUS: Tunnel-Type [64] 6 01:ESP [9]
1w0d: RADIUS: Tunnel-Password [69] 21 *
1w0d: RADIUS: saved authorization data for user 830CAF28 at 83143E64
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=ike"
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=preshared-key"
1w0d: RADIUS: cisco AVPair "ipsec:addr-pool=ippool"
1w0d: RADIUS: cisco AVPair "ipsec:inac1=108"
1w0d: RADIUS: Tunnel-Type, [01] 00 00 09
1w0d: RADIUS: TAS(1) created and enqueued.
1w0d: RADIUS: Tunnel-Password decrypted, [01] cisco123
1w0d: RADIUS: TAS(1) takes precedence over tagged attributes,
tunnel_type=esp
1w0d: RADIUS: free TAS(1)
1w0d: AAA/AUTHOR (3098118746): Post authorization status = PASS_REPL
1w0d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV key-exchange=preshared-key
AAA/AUTHOR/IKE: Processing AV addr-pool=ippool
AAA/AUTHOR/IKE: Processing AV inac1=108
AAA/AUTHOR/IKE: Processing AV tunnel-type*esp
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV tunnel-tag*1
1w0d: ISAKMP (0:2): attributes sent in message:
1w0d: Address: 0.2.0.0
1w0d: ISAKMP (0:2): allocating address 10.16.20.2
1w0d: ISAKMP: Sending private address: 10.16.20.2
1w0d: ISAKMP: Unknown Attr: IP4_NETMASK (0x2)
1w0d: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address:
86395
1w0d: ISAKMP: Sending APPLICATION_VERSION string: Cisco Internetwork
Operating System Software
IOS (tm) C2600 Software (C2600-JK9O3S-M), Version 12.2(8)T, RELEASE
SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 14-Feb-02 16:50 by ccai
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7000)
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7001)
1w0d: ISAKMP: Sending split include name 108 network 14.38.0.0 mask
255.255.0.0 protocol 0, src port 0, dst port 0

1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7007)
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7008)
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7005)
1w0d: ISAKMP (0:2): responding to peer config from 10.0.0.1. ID =
-1911189201
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) CONF_ADDR
1w0d: ISAKMP (0:2): deleting node -1911189201 error FALSE reason ""
1w0d: ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR
Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

1w0d: AAA/MEMORY: free_user (0x830CAF28) user='3000client' ruser='NULL'
port='ISAKMP-GROUP-AUTH' rem_addr='10.0.0.1' authen_type=NONE
service=LOGIN priv=0
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): processing HASH payload. message ID = 132557281
1w0d: ISAKMP (0:2): processing SA payload. message ID = 132557281
1w0d: ISAKMP (0:2): Checking IPsec proposal 1
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-MD5
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
```

1w0d: IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 1) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): skipping next ANDeD proposal (1)  
1w0d: ISAKMP (0:2): Checking IPsec proposal 2  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-SHA  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: ISAKMP (0:2): atts are acceptable.  
1w0d: ISAKMP (0:2): Checking IPsec proposal 2  
1w0d: ISAKMP (0:2): transform 1, IPPCP LZS  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 4, trans 3, hmac\_alg 0) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): Checking IPsec proposal 3  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-MD5  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 1) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): Checking IPsec proposal 4  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-SHA  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
**1w0d: ISAKMP (0:2): atts are acceptable.**  
1w0d: IPSEC(validate\_proposal\_request): proposal part #1,  
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,  
local\_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1),  
remote\_proxy= 10.16.20.2/255.255.255.255/0/0 (type=1),  
protocol= ESP, transform= esp-3des esp-sha-hmac ,  
lifedur= 0s and 0kb,  
spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4  
1w0d: ISAKMP (0:2): processing NONCE payload. message ID = 132557281  
1w0d: ISAKMP (0:2): processing ID payload. message ID = 132557281  
1w0d: ISAKMP (0:2): processing ID payload. message ID = 132557281  
1w0d: ISAKMP (0:2): asking for 1 spis from ipsec  
1w0d: ISAKMP (0:2): Node 132557281, Input = IKE\_MSG\_FROM\_PEER,  
IKE\_QM\_EXCH  
Old State = IKE\_QM\_READY New State = IKE\_QM\_SPI\_STARVE  
  
1w0d: IPSEC(key\_engine): got a queue event...  
1w0d: IPSEC(spi\_response): getting spi 245824456 for SA  
from 10.1.1.1 to 10.0.0.1 for prot 3  
1w0d: ISAKMP: received ke message (2/1)  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM\_IDLE  
1w0d: ISAKMP (0:2): Node 132557281, Input = IKE\_MSG\_FROM\_IPSEC,  
IKE\_SPI\_REPLY  
Old State = IKE\_QM\_SPI\_STARVE New State = IKE\_QM\_R\_QM2  
  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM\_IDLE

```
1w0d: ISAKMP (0:2): Creating IPsec SAs
1w0d: inbound SA from 10.0.0.1 to 10.1.1.1
(proxy 10.16.20.2 to 10.1.1.1)
1w0d: has spi 0xEA6FBC8 and conn_id 2000 and flags 4
1w0d: lifetime of 2147483 seconds
1w0d: outbound SA from 10.1.1.1 to 10.0.0.1 (proxy
10.1.1.1 to 10.16.20.2 )
1w0d: has spi 1009463339 and conn_id 2001 and flags C
1w0d: lifetime of 2147483 seconds
1w0d: ISAKMP (0:2): deleting node 132557281 error FALSE reason "quick mode
done (await())"
1w0d: ISAKMP (0:2): Node 132557281, Input = IKE_MSG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

1w0d: IPSEC(key_engine): got a queue event...
1w0d: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,
local_proxy= 10.1.1.1/0.0.0.0/0/0 (type=1),
remote_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 2147483s and 0kb,
spi= 0xEA6FBC8(245824456), conn_id= 2000, keysize= 0, flags= 0x4
1w0d: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.1.1.1, remote= 10.0.0.1,
local_proxy= 10.1.1.1/0.0.0.0/0/0 (type=1),
remote_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x3C2B302B(1009463339), conn_id= 2001, keysize= 0, flags= 0xC
1w0d: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.1.1, sa_prot= 50,
sa_spi= 0xEA6FBC8(245824456),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2000
1w0d: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.0.0.1, sa_prot= 50,
sa_spi= 0x3C2B302B(1009463339),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2001
1w0d: ISAKMP: received ke message (4/1)
1w0d: ISAKMP: Locking CONFIG struct 0x830BF118 for
crypto_ikmp_config_handle_kei_mess, count 3
1w0d: ISAKMP (0:1): purging SA., sa=83196748, delme=83196748
1w0d: ISAKMP: Unlocking CONFIG struct 0x830BF118 on return of attributes,
count 2
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): processing HASH payload. message ID = -1273332908
1w0d: ISAKMP (0:2): processing SA payload. message ID = -1273332908
1w0d: ISAKMP (0:2): Checking IPsec proposal 1
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-MD5
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3,
hmac_alg 1) not supported
1w0d: ISAKMP (0:2):atts not acceptable. Next payload is 0
1w0d: ISAKMP (0:2): skipping next ANDed proposal (1)
1w0d: ISAKMP (0:2): Checking IPsec proposal 2
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-SHA
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
```

1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: ISAKMP (0:2): atts are acceptable.  
1w0d: ISAKMP (0:2): Checking IPsec proposal 2  
1w0d: ISAKMP (0:2): transform 1, IPPCP LZS  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 4, trans 3, hmac\_alg 0) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): Checking IPsec proposal 3  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-MD5  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 1) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): Checking IPsec proposal 4  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-SHA  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: ISAKMP (0:2): atts are acceptable.  
1w0d: IPSEC(validate\_proposal\_request): proposal part #  
vpn2611#1,  
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,  
local\_proxy= 14.38.0.0/255.255.0.0/0/0 (type=4),  
remote\_proxy= 10.16.20.2/255.255.255.255/0/0 (type=1),  
protocol= ESP, transform= esp-3des esp-sha-hmac ,  
lifedur= 0s and 0kb,  
spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4  
1w0d: ISAKMP (0:2): processing NONCE payload. message ID = -1273332908  
1w0d: ISAKMP (0:2): processing ID payload. message ID = -1273332908  
1w0d: ISAKMP (0:2): processing ID payload. message ID = -1273332908  
1w0d: ISAKMP (0:2): asking for 1 spis from ipsec  
1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE\_MSG\_FROM\_PEER,  
IKE\_QM\_EXCH  
Old State = IKE\_QM\_READY New State = IKE\_QM\_SPI\_STARVE  
  
1w0d: IPSEC(key\_engine): got a queue event...  
1w0d: IPSEC(spi\_response): getting spi 593097454 for SA  
from 10.1.1.1 to 10.0.0.1  
vpn2611#  
vpn2611#2 for prot 3  
1w0d: ISAKMP: received ke message (2/1)  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM\_IDLE  
1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE\_MSG\_FROM\_IPSEC,  
IKE\_SPI\_REPLY  
Old State = IKE\_QM\_SPI\_STARVE New State = IKE\_QM\_R\_QM2  
  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM\_IDLE  
**1w0d: ISAKMP (0:2): Creating IPsec SAs**  
**1w0d: inbound SA from 10.0.0.1 to 10.1.1.1**  
**(proxy 10.16.20.2 to 14.38.0.0)**  
**1w0d: has spi 0x2359F2EE and conn\_id 2002 and flags 4**  
**1w0d: lifetime of 2147483 seconds**  
**1w0d: outbound SA from 10.1.1.1 to 10.0.0.1 (proxy**  
**14.38.0.0 to 10.16.20.2 )**

```
lw0d: has spi 1123818858 and conn_id 2003 and flags C
lw0d: lifetime of 2147483 seconds
lw0d: ISAKMP (0:2): deleting node -1273332908 erro
vpn2611#un ar FALSE reason "quick mode done (await())"
lw0d: ISAKMP (0:2): Node -1273332908, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

lw0d: IPSEC(key_engine): got a queue event...
lw0d: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,
local_proxy= 172.18.124..0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x2359F2EE(593097454), conn_id= 2002, keysize= 0, flags= 0x4
lw0d: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.1.1.1, remote= 10.0.0.1,
local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sh11
All possible debugging has been turned off
vpn2611#a-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x42FC1D6A(1123818858), conn_id= 2003, keysize= 0, flags= 0xC
lw0d: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.1.1, sa_prot= 50,
sa_spi= 0x2359F2EE(593097454),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2002
lw0d: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.0.0.1, sa_prot= 50,
sa_spi= 0x42FC1D6A(1123818858),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2003
```

## [Informações Relacionadas](#)

- [Suporte por tecnologia do RAO](#)
- [Apoio da Negociação IPSec/Protocolos IKE](#)
- [Sustentação do produto do Cisco VPN Client](#)
- [Request For Comments \(RFC\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)