

Настройка IPSec между маршрутизатором Cisco IOS и Cisco VPN Client 4.x for Windows с использованием RADIUS

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Теоретические сведения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Конфигурация сервера RADIUS](#)

[Проверка](#)

[Устранение неполадок](#)

[Команды для устранения неполадок](#)

[Выходные данные отладки](#)

[Дополнительные сведения](#)

Введение

Этот документ демонстрирует настройку соединения между маршрутизатором Cisco IOS и VPN-клиентом Cisco 4.x с использованием RADIUS для авторизации групп и аутентификации пользователей. Выпуск ПО Cisco IOS® 12.2(8)T и последующие выпуски поддерживают подключения от клиентов Cisco VPN Client 3.x. В клиентах VPN Client 3.x и 4.x используются политики группы 2 Диффи-Хелмана (DH). Команда `isakmp policy # group 2` разрешает подключение VPN-клиентов.

Примечание: Учет IPSEC VPN теперь доступен. [Дополнительные сведения и примеры конфигураций см. в документе Учет IPsec VPN.](#)

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Для IPSec выделен пул адресов
- Группа звонила "3000clients" с предварительным общим ключом "cisco123"
- Авторизация группы и проверка подлинности пользователя на сервере RADIUS

Примечание: При этом не поддерживается RADIUS Accounting.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Маршрутизатор 2611, использующий программное обеспечение Cisco IOS Software Release 12.2(8)T.
- Cisco Secure ACS для Windows (любой сервер RADIUS должен работать),
- Cisco VPN Client для Версии Windows 4.8 (любой Клиент VPN 4.x должен работать),

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Результат выполнения команды show version на маршрутизаторе:

```
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
```

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

Теоретические сведения

Этот документ показывает проверку подлинности и авторизация, такую как присвоение Сервиса Windows назначения имен в интернете (WINS) и Domain Naming Service (DNS), сервером RADIUS. [Если вы заинтересованы в выполнении аутентификации на сервере RADIUS и авторизации, произведенной локально маршрутизатором, см. документ Настройка IPSec между маршрутизатором Cisco IOS и Cisco VPN Client 4.x for Windows с использованием RADIUS для аутентификации пользователей.](#)

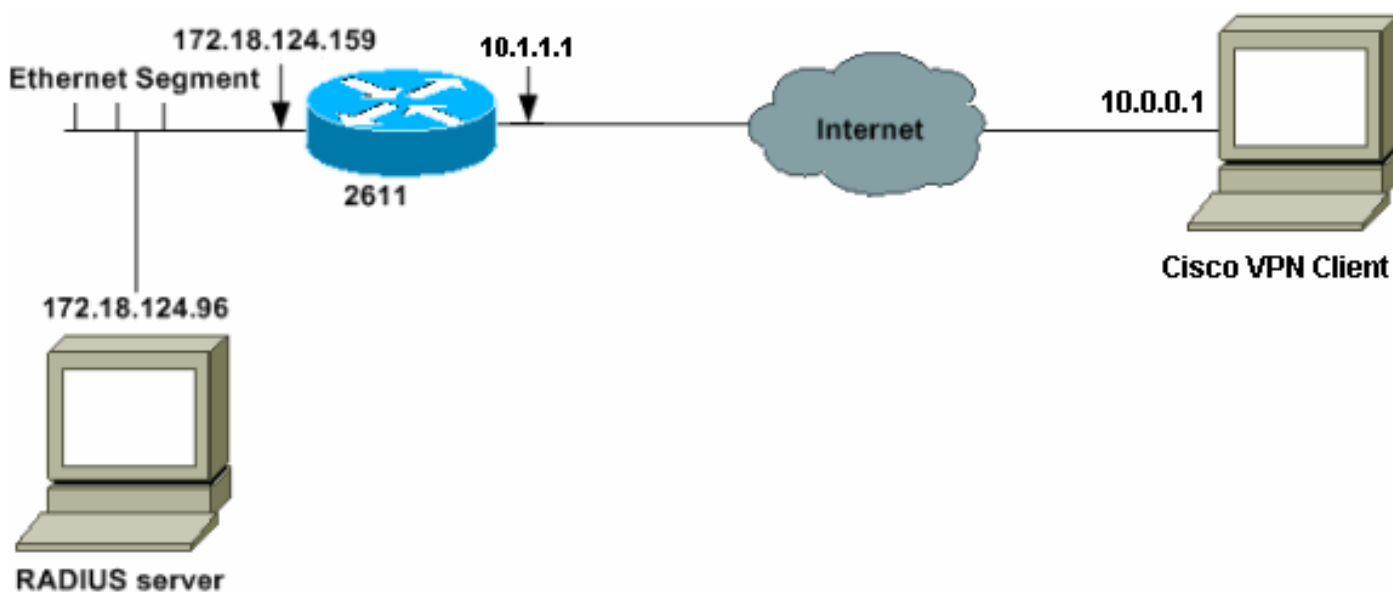
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: [Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд \(только для зарегистрированных клиентов\).](#)

Схема сети

В настоящем документе используется следующая схема сети:



Примечание: IP-адреса в сети данного примера не маршрутизуемы в глобальной сети Интернет, потому что они - закрытые IP - адреса в лабораторной сети.

Конфигурации

Маршрутизатор 2611

```
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
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
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#
```

[Конфигурация сервера RADIUS](#)

[Настройте сервер RADIUS для клиентов AAA \(маршрутизатор\)](#)

Выполните следующие действия:

1. **Нажмите Add Запись** для добавления маршрутизатора к Базе данных сервера RADIUS.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
340	172.18.124.151	RADIUS (Cisco Aironet)
Aironet-340-Lab	14.36.1.99	RADIUS (Cisco Aironet)
glenntest	172.18.124.120	RADIUS (Cisco IOS/PIX)
router	172.18.124.150	TACACS+ (Cisco IOS)

- [Network Device Groups](#)
- [Adding a Network Device Group](#)
- [Renaming a Network Device Group](#)
- [Deleting a Network Device Group](#)
- [AAA Clients](#)
- [Adding a AAA Client](#)
- [Editing a AAA Client](#)
- [Deleting a AAA Client](#)
- [AAA Servers](#)
- [Adding a AAA Server](#)
- [Editing a AAA Server](#)
- [Deleting a AAA Server](#)
- [Proxy Distribution Table](#)
- [Adding a Proxy Distribution Table Entry](#)
- [Sorting Proxy Distribution Table Entries](#)

2. Установите IP-адрес маршрутизатора 172.18.124.159, а также общий секретный ключ "cisco123" и выберите RADIUS в раскрывающемся меню Authenticate Using.

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Key:

Authenticate Using:

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

[Submit] [Submit + Restart] [Cancel]

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

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

AAA Client IP Address

[Настройте сервер RADIUS для групповой аутентификации и авторизации](#)

Выполните следующие действия:

1. Нажмите **Add/Edit** для добавления Пользователя, названного **3000client** к серверу RADIUS.

User:

List users beginning with letter/number:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9																

- [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, delete users in the database.

User Setup and External User Databases

Before Cisco Secure ACS can authenticate users with an external user database, you must:

- You must have the database up and running on the external server. For example, if you are using token card authentication, you must have the database up and running and properly configured.
- You must have configured the applicable parameters in the Cisco Secure ACS configuration.

2. Установите пароль **cisco** для этого пользователя. Этот пароль является специальным ключевым словом для Cisco IOS, которая указывает, что нужно сослаться на профиль группы. Если вы предпочитаете, можно сопоставить пользователя с группой Cisco Secure. Удостоверьтесь, что выбрано присвоение **No IP**

address.

CISCO SYSTEMS

User Setup

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. Задайте параметры авторизации группы, которые будут переданы этой учетной записью пользователя назад Клиенту VPN. **Убедитесь, что у вас включен cisco-av-pair со следующими атрибутами:** iPsec: key-exchange=ike iPsec: key-exchange=preshared-key iPsec: addr-pool=ippool iPsec: inacl=108 (только необходимый, если вы используете разделенное туннелирование на маршрутизаторе), Также убедитесь, что атрибуты heseg IETF RADIUS Attributes включены (задействованы): Атрибут 6: Service-Type=Outbound Атрибут 64: Tunnel-Type=IP ESP Атрибут 69: Tunnel-Password=cisco123

(это - ваш пароль группы на Клиенте VPN), По завершении нажмите кнопку Submit (Отправить).

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:inac1=10e
```

IETF RADIUS Attributes ?

[006] Service-Type

[007] Framed-Protocol

[027] Session-Timeout

[028] Idle-Timeout

[064] Tunnel-Type

Tag Value

Tag Value

[069] Tunnel-Password

Tag Value


Tag Value

Под Определяемыми поставщиком Атрибутами можно также включить эти необязательные атрибуты: iPSec: домен по умолчанию = iPSec: таймаут = iPSec: idletime = iPSec: серверы dns = iPSec: серверы wins =

[Настройка сервера RADIUS для аутентификации пользователей](#)

Выполните следующие действия:

1. Нажмите **Add/Edit** для добавления пользователя VPN в базе данных Cisco Secure. В этом примере имя пользователя –cisco.



User:

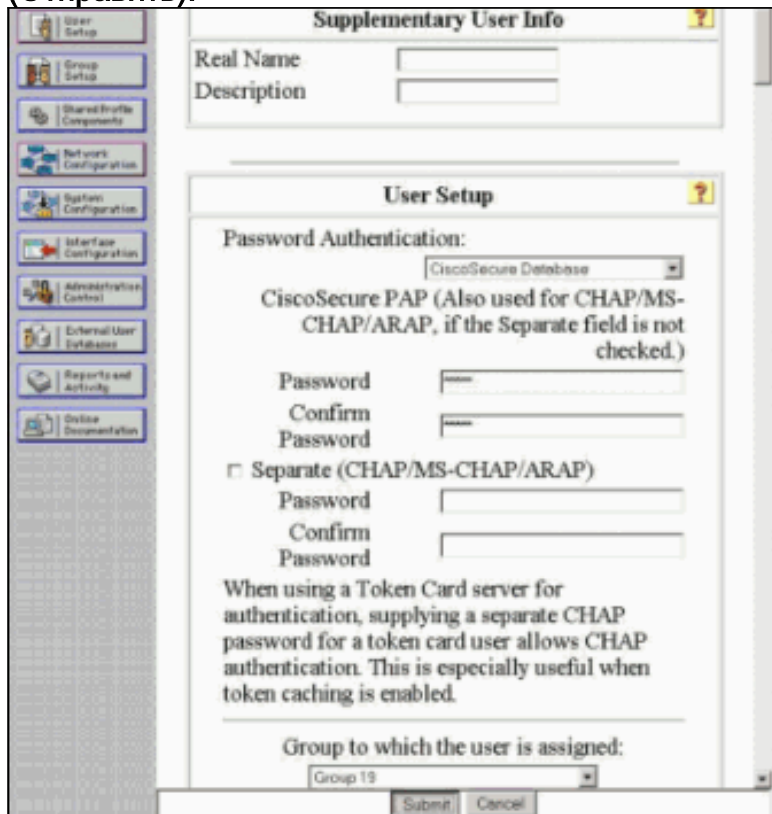
List users beginning with letter/number:

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

- [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. В следующем окне определите пароль для пользователя cisco. Пароль является также Cisco. Учетную запись пользователя можно включить в группу. По завершении нажмите кнопку **Submit** (Отправить).



Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

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:

- [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

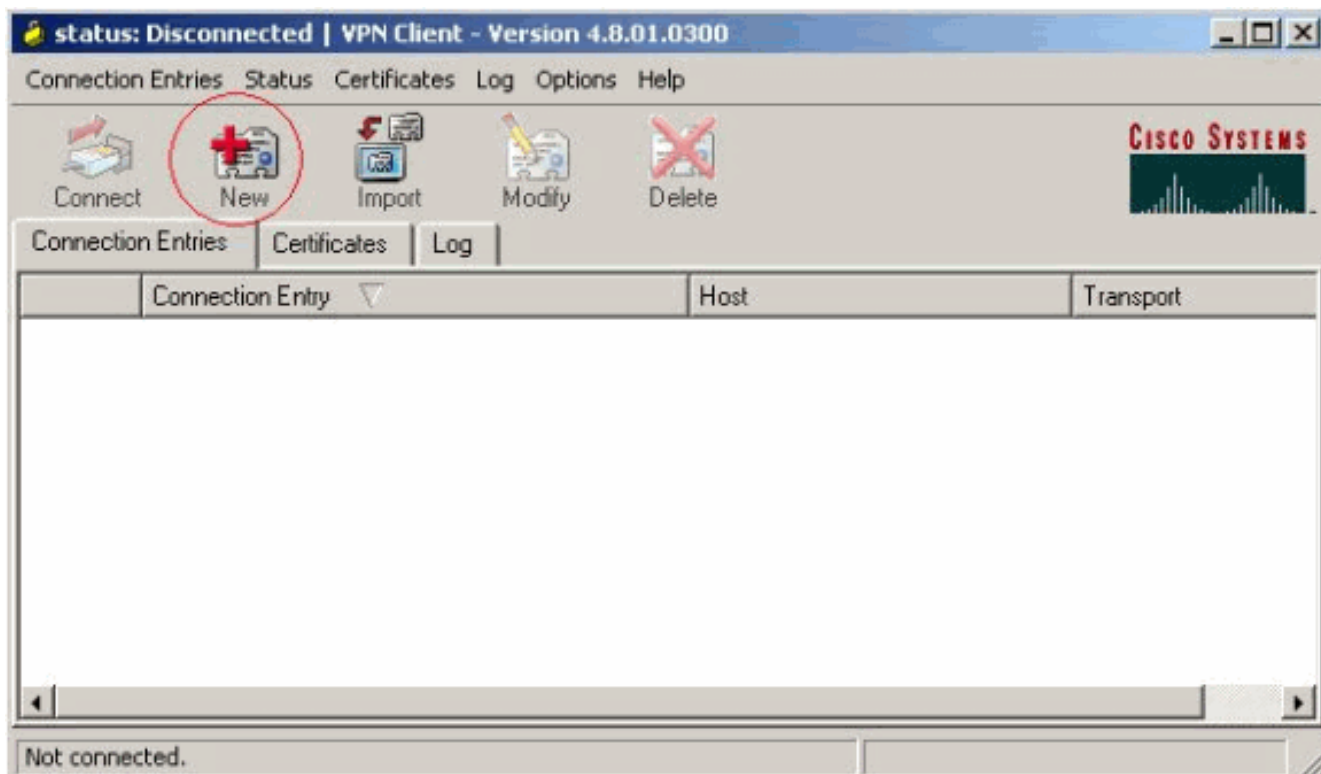
Select the Account Disabled check box to disable this account; clear the check box to enable the account.

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

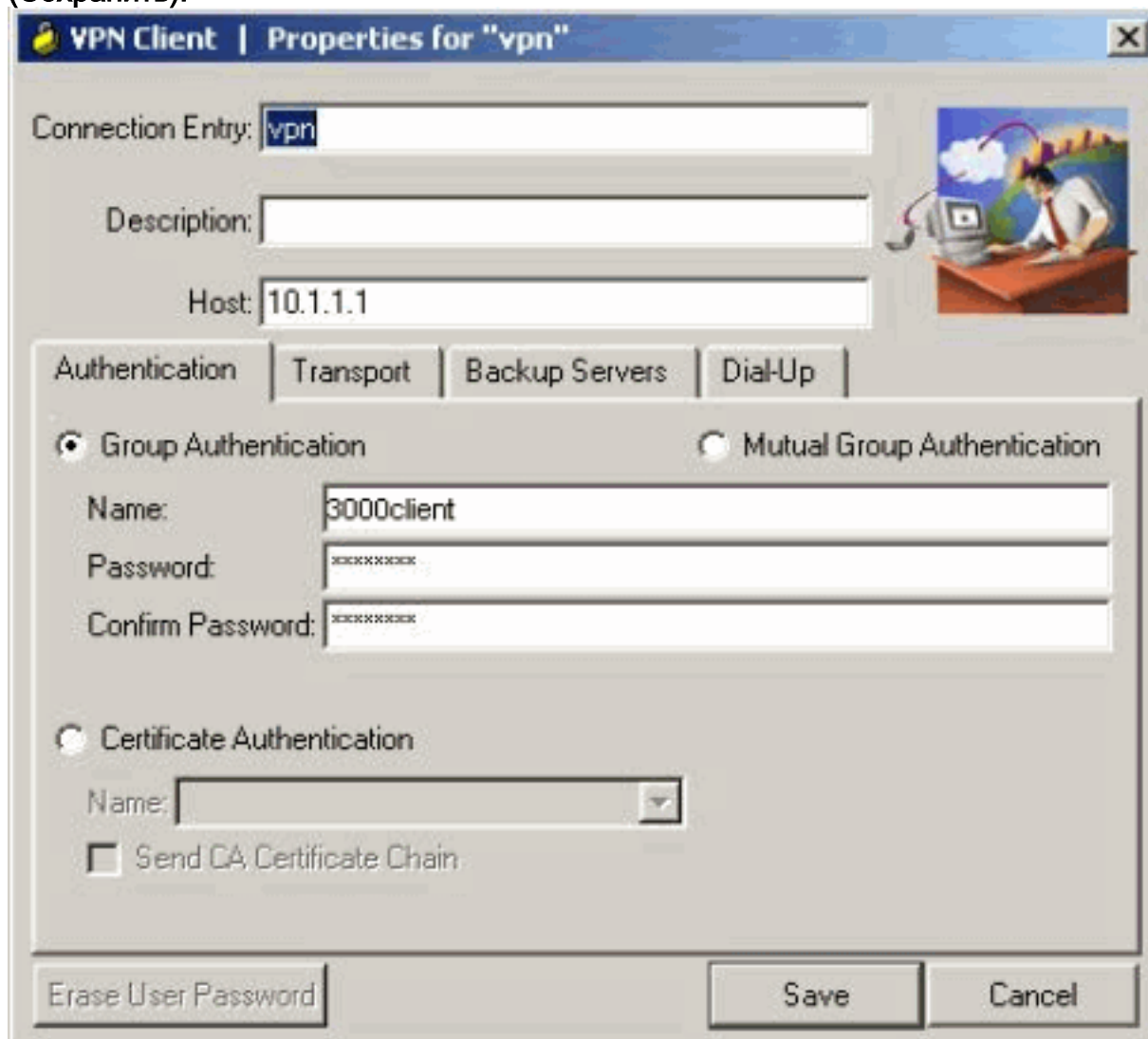
[Настройка VPN Client 4.8](#)

Чтобы настроить VPN Client 4.8, выполните следующие действия:

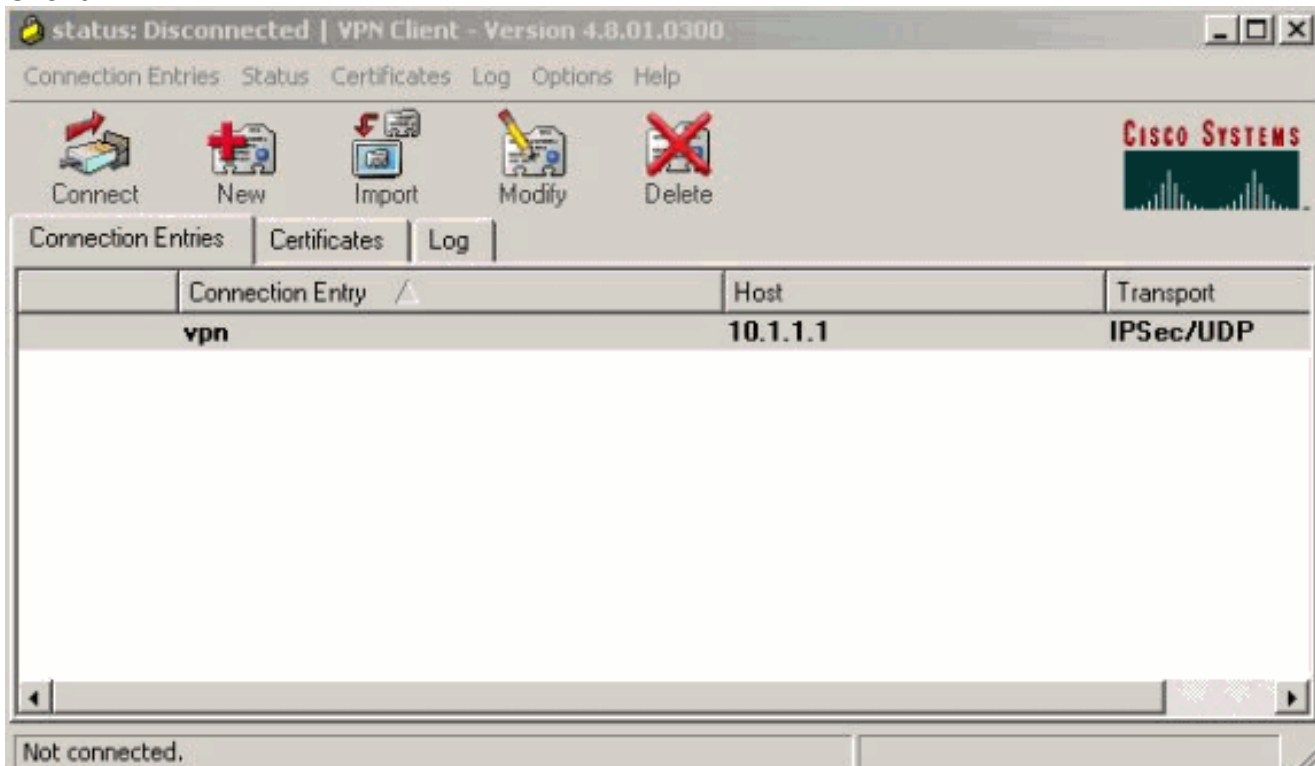
1. Выберите Пуск > Программы > Cisco Systems VPN Client > VPN Client.
2. Нажмите кнопку New (Создать), чтобы открыть окно Create New VPN Connection Entry (Создание записи нового VPN-подключения).



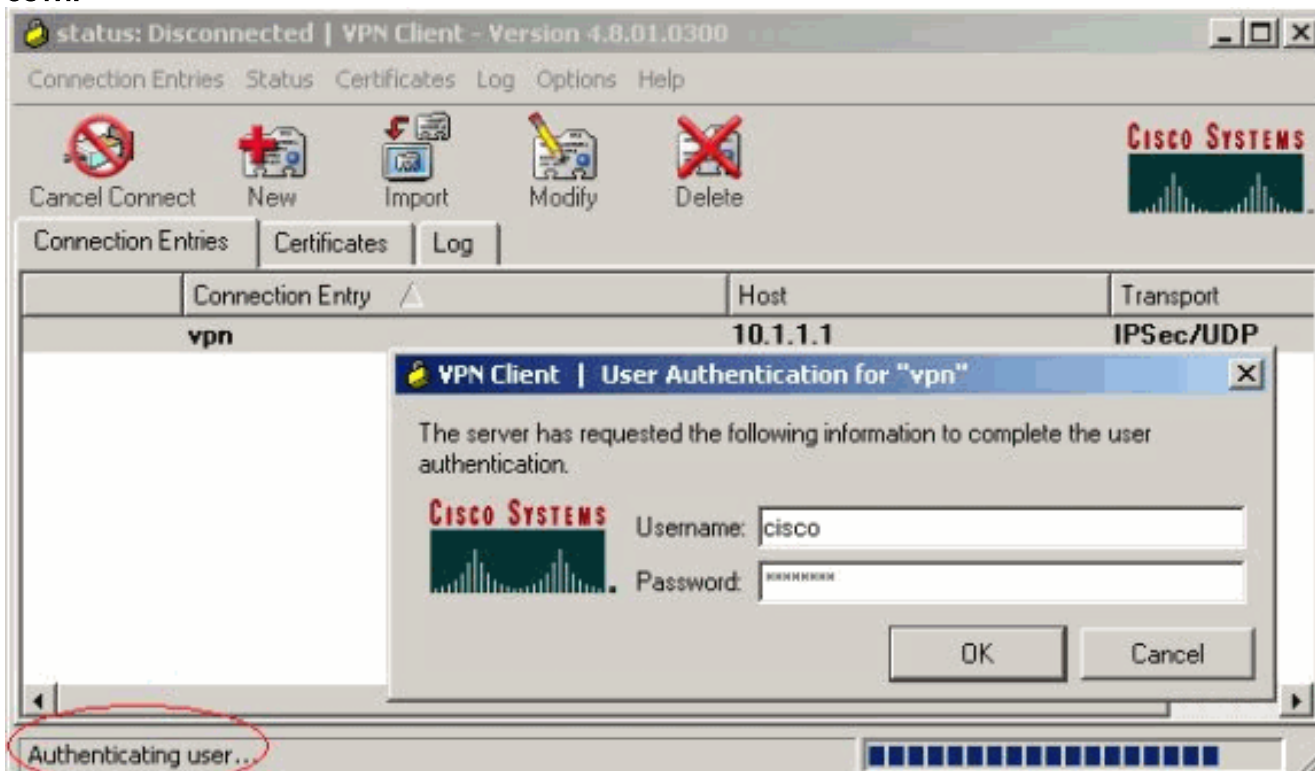
3. Введите имя записи и описание подключения. Введите внешний IP-адрес маршрутизатора в поле Host (Хост). Затем введите имя группы VPN и нажмите кнопку Save (Сохранить).



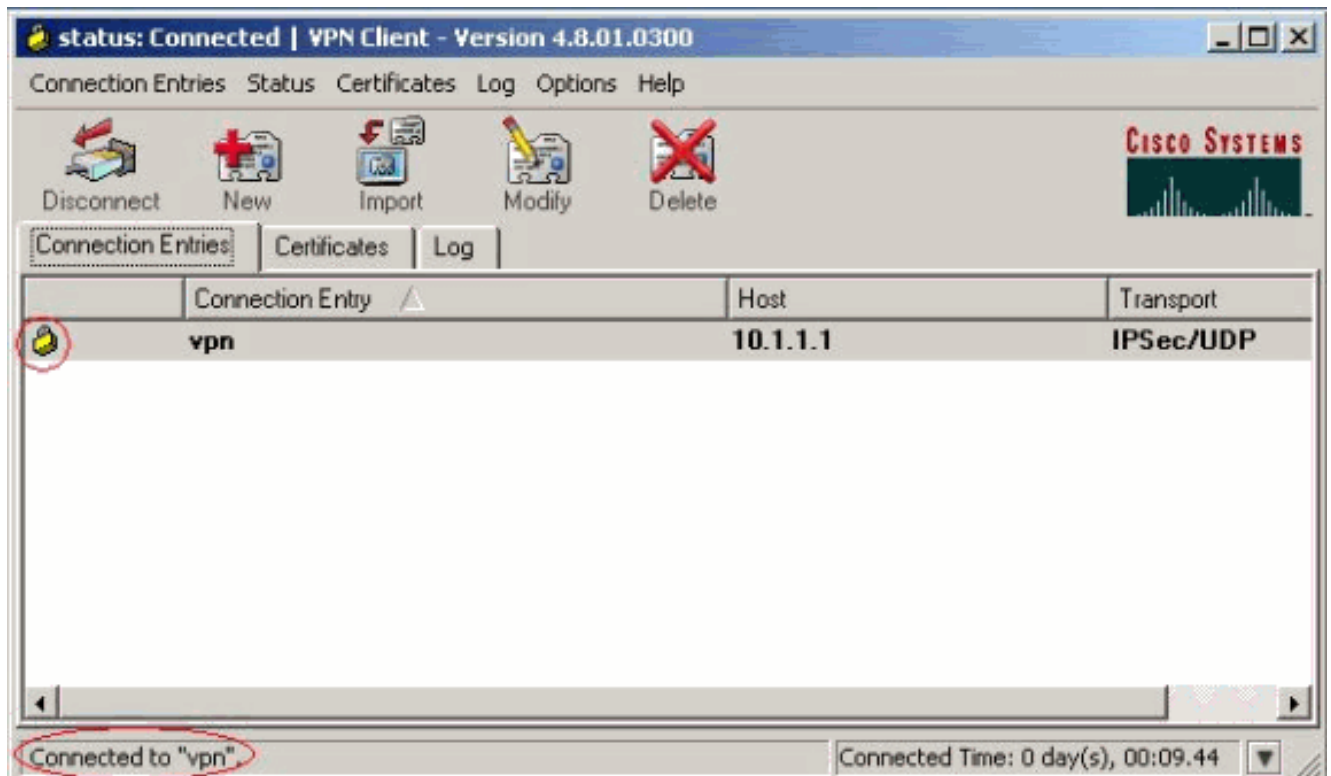
4. Щелкните по соединению, вы хотите использовать и нажать **Connect** от главного окна VPN Client.



5. При появлении соответствующего запроса введите имя пользователя и пароль для аутентификации Xauth и нажмите ОК для подключения к удаленной сети.



ПО VPN Client соединится с маршрутизатором на центральном узле.



Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

[Средство Output Interpreter \(OIT\)](#) (только для зарегистрированных клиентов) поддерживает [определенные команды show](#). Посредством OIT можно анализировать выходные данные команд `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

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. Посредством OIT можно анализировать выходные данные команд show.

Примечание: Прежде чем выполнять какие-либо команды отладки, ознакомьтесь с документом "Важные сведения о командах отладки".

- debug crypto ipsec - отображаются данные отладки подключений IPsec.
- debug crypto isakmp— отображает данные отладки подключений IPsec и первый набор атрибутов, отклоняемых из-за несовместимости на обоих концах.
- debug crypto engine— выводит информацию о криптографическом модуле.
- debug aaa authentication — отображаются сведения при аутентификации AAA/TACACS+.
- debug aaa authorization – отображает сведения об авторизации AAA/TACACS+.
- debug radius — отображает диагностические сведения об обмене данными между сервером RADIUS и маршрутизатором.

Выходные данные отладки

В этом разделе содержатся отладочные сведения маршрутизатора, которые можно использовать для устранения неполадок конфигурации.

Журналы маршрутизатора

```
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

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 )
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
```

[Журналы клиента](#)

Для просмотра журналов запустите на VPN-клиенте средство LogViewer. Убедитесь в том, что для всех настроенных классов установлена высокая фильтрация (High). Ниже показан пример журнала:

```
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-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_MESG_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

[Дополнительные сведения](#)

- [Поддержка технологии RADIUS](#)
- [Страница поддержки IPsec Negotiation/IKE](#)
- [Клиент Cisco VPN – Поддержка продукта](#)
- [Запрос на комментарии \(RFC\)](#)
- [Cisco Systems – техническая поддержка и документация](#)