

# Пример конфигурации туннеля IPsec между маршрутизатором IOS и Cisco VPN Client 4.x для Windows с проверкой подлинности пользователя TACACS +

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Проверка](#)

[Устранение неполадок](#)

[Команды для устранения неполадок](#)

[Журналы маршрутизатора](#)

[Журналы клиента](#)

[Дополнительные сведения](#)

## Введение

В этом документе описана настройка соединения IPsec между маршрутизатором и клиентом Cisco VPN Client 4.x с использованием службы TACACS+ для аутентификации пользователей. Выпуск Cisco IOS® 12.2(8)T и последующие версии поддерживают входящие подключения клиента Cisco VPN Client 4.x. Клиент VPN Client 4.x использует политику группы 2 Диффи-Хелмана (DH). Подключение клиентов 4.x разрешается командой `isakmp policy # group 2`.

Этот документ иллюстрирует аутентификацию на сервере TACACS+ с авторизацией, выполняемой на маршрутизаторе локально, например назначениями служб имен WINS и DNS.

[Подробную информацию о сценарии, в котором аутентификация пользователя выполняется локально на маршрутизаторе Cisco IOS, см. в документе Настройка VPN-клиента Cisco VPN Client 3.x для подключения из Windows к IOS с использованием локальной аутентификации.](#)

[Другой сценарий, в котором аутентификация пользователя выполняется с помощью протокола RADIUS, см. в документе Настройка обмена данными по IPsec-протоколу между маршрутизатором под управлением операционной системы Cisco IOS и Cisco VPN Client 4.x для Windows с использованием аутентификации пользователей по протоколу RADIUS.](#)

# Предварительные условия

## Требования

Прежде чем использовать эту конфигурацию, убедитесь, что выполняются следующие требования:

- Для IPSec выделен пул адресов
- Имеется группа vpngroup с паролем cisco123
- Аутентификация пользователей выполняется на сервере TACACS+

## Используемые компоненты

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

- Клиент Cisco VPN Client для Windows версии 4.0.2D (должны работать любые клиенты VPN Client 3.x и последующих версий).
- Cisco Secure for Windows версии 3.0 (подходит любой сервер TACACS+)
- Маршрутизатор Cisco IOS 1710 версии 12.2(8)T1 с загруженным набором функций IPSec

**Ниже приведены результаты выполнения команды show version в маршрутизаторе.**

```
1710#show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1710-K9O3SY-M),
  Version 12.2(8)T1, RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 30-Mar-02 13:30 by ccai
Image text-base: 0x80008108, data-base: 0x80C1E054
```

```
ROM: System Bootstrap, Version 12.2(1r)XE1, RELEASE SOFTWARE (fc1)
```

```
1710 uptime is 1 week, 6 days, 22 hours, 30 minutes
System returned to ROM by reload
System image file is "flash:c1710-k9o3sy-mz.122-8.T1"
```

```
cisco 1710 (MPC855T) processor (revision 0x200)
  with 27853K/4915K bytes of memory.
Processor board ID JAD052706CX (3234866109), with hardware revision 0000
MPC855T processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 Virtual Private Network (VPN) Module(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
```

```
Configuration register is 0x2102
```

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.

## Условные обозначения

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

## 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:** Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. [Это адреса RFC 1918, которые использовались в лабораторной среде.](#)

## Конфигурации

Эти конфигурации используются в данном документе:

- [Маршрутизатор Cisco 1710](#)
- [Сервер TACACS+](#)
- [VPN Client 4.x](#)
- [Раздельное туннелирование](#)

## Маршрутизатор Cisco 1710

### Маршрутизатор Cisco 1710

```
1710#show run
Building configuration...

Current configuration : 1884 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1710
!
!--- Enable authentication, authorization and accounting
(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. !--- The group TACACS+ command
specifies TACACS+ user authentication.
```

```
aaa authentication login userauthen group tacacs+
!--- In order to enable group authorization, !--- enable
the aaa authorization commands.

aaa authorization network groupauthor local
!
!
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 a group in order to specify the !--- WINS
and DNS server addresses to the VPN Client, !--- along
with the pre-shared key for authentication. crypto
isakmp client configuration group vpngroup
key cisco123
dns 10.2.1.10
wins 10.2.1.20
domain cisco.com
pool ippool
!
!--- 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 previously 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 FastEthernet0
ip address 172.18.124.158 255.255.255.0
crypto map clientmap
!
interface Ethernet0
ip address 10.38.50.51 255.255.0.0
!
```

```
!--- Create a pool of addresses to be assigned to the
VPN Clients. ip local pool ippool 10.1.1.100 10.1.1.200
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip route 172.16.124.0 255.255.255.0 10.38.1.1
ip route 10.2.1.0 255.255.255.0 10.38.1.1
ip http server
ip pim bidir-enable
!
!
!
!--- Specify the IP address of the TACACS+ server, !---
along with the TACACS+ shared secret key. tacacs-server
host 172.16.124.96 key cisco123
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end
```

## Сервер TACACS+

Чтобы настроить сервер TACACS+, выполните следующие действия:

1. Выберите **Add Entry (Добавить запись)**, чтобы добавить запись для маршрутизатора в серверную базу данных TACACS+.
2. На странице **Add AAA Client (Добавление клиента AAA)** введите сведения о маршрутизаторе, как показано на рисунке: В поле **AAA Client Hostname (Имя хоста клиента AAA)** введите имя маршрутизатора. В поле **AAA Client IP Address (IP-адрес клиента AAA)** введите 10.38.50.51. В поле **Key (Ключ)** введите общий секретный ключ: cisco123. Из "Authenticate", используя ниспадающий список, выберите TACACS+(Cisco IOS), и нажмите **Submit**.
3. В поле **User (Пользователь)** введите имя пользователя VPN в базе данных службы Cisco Secure, затем нажмите **Add/Edit (Добавить/редактировать)**. В этом примере имя пользователя –cisco.
4. На следующей странице введите и подтвердите пароль пользователя cisco. В данном примере пароль – также cisco.
5. Если нужно привязать учетную запись пользователя к группе, выполните это действие сейчас. По завершении нажмите кнопку **Submit (Отправить)**.

## VPN Client 4.x

Для настройки клиента VPN Client 4.x выполните следующие действия:

1. Запустите **VPN Client**, а затем нажмите кнопку **New (Создать)**, чтобы создать новое подключение. В клиенте VPN Client откроется диалоговое окно **Create New VPN Connection Entry (Создание записи нового подключения VPN)**.
2. В диалоговом окне **Create New VPN Connection Entry (Создание записи нового подключения VPN)** введите информацию о подключении, как показано на рисунке: В

поле Connection Entry (Запись подключения) введите имя подключения. В полях Description (Описание) и Host (Хост) введите описание и IP-адрес хоста для записи подключения. На вкладке Authentication (Аутентификация) выберите переключатель Group Authentication (Аутентификация группы) и введите имя и пароль пользователя. Для сохранения подключения нажмите кнопку Save (Сохранить).

3. В окне VPN Client выберите созданную запись подключения и нажмите кнопку Connect (Подключить), чтобы подключиться к маршрутизатору.
4. Во время согласования протокола IPsec будет предложено ввести имя пользователя и пароль. Введите имя пользователя и пароль. В окне будут отображены следующие сообщения: Negotiating security profiles (Согласование профилей безопасности). "Your link is now secure (Соединение переведено в защищенный режим)."

## Раздельное туннелирование

Чтобы разрешить раздельное туннелирование для VPN-подключений, убедитесь, что в маршрутизаторе настроен список контроля доступа. В нижеследующем примере команда `access-list 102` связана с группой для раздельного туннелирования, и формируется туннель с сетями 10.38.X.X /16 и 10.2.x.x. К устройствам не в ACL 102 (например, в интернете) трафик течет незашифрованным.

```
access-list 102 permit ip 10.38.0.0 0.0.255.255 10.1.1.0 0.0.0.255
access-list 102 permit ip 10.2.0.0 0.0.255.255 10.1.1.0 0.0.0.255
```

Применение ACL к свойствам группы.

```
crypto isakmp client configuration group vpngroup
key cisco123
dns 10.2.1.10
wins 10.2.1.20
domain cisco.com
pool ippool
acl 102
```

## Проверка

В данном разделе содержатся сведения для проверки работы текущей конфигурации.

Некоторые команды `show` поддерживаются интерпретатором выходных данных (только для зарегистрированных пользователей). Этот инструмент позволяет просмотреть анализ выходных данных команды `show`.

```
1710#show crypto isakmp sa
dst          src          state          conn-id      slot
172.18.124.158 192.168.60.34 QM_IDLE        3            0
```

```
1710#show crypto ipsec sa
```

```
interface: FastEthernet0
Crypto map tag: clientmap, local addr. 172.18.124.158
```

```
local ident (addr/mask/prot/port): (172.18.124.158/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.1.1.114/255.255.255.255/0/0)
current_peer: 192.168.60.34
```

PERMIT, flags={}  
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0  
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0  
#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.: 172.18.124.158, remote crypto endpt.: 192.168.60.34  
path mtu 1500, media mtu 1500  
current outbound spi: 8F9BB05F

inbound esp sas:  
spi: 0x61C53A64(1640315492)  
transform: esp-3des esp-sha-hmac ,  
in use settings ={Tunnel, }  
slot: 0, conn id: 200, flow\_id: 1, crypto map: clientmap  
sa timing: remaining key lifetime (k/sec): (4608000/3294)  
IV size: 8 bytes  
replay detection support: Y

inbound ah sas:

inbound pcsp sas:

outbound esp sas:  
spi: 0x8F9BB05F(2409345119)  
transform: esp-3des esp-sha-hmac ,  
in use settings ={Tunnel, }  
slot: 0, conn id: 201, flow\_id: 2, crypto map: clientmap  
sa timing: remaining key lifetime (k/sec): (4608000/3294)  
IV size: 8 bytes  
replay detection support: Y

outbound ah sas:

outbound pcsp sas:

local ident (addr/mask/prot/port): (10.38.0.0/255.255.0.0/0/0)  
remote ident (addr/mask/prot/port): (10.1.1.114/255.255.255.255/0/0)  
**current\_peer: 192.168.60.34**

PERMIT, flags={}  
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3  
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3  
#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.: 172.18.124.158, remote crypto endpt.: 192.168.60.34  
path mtu 1500, media mtu 1500  
current outbound spi: 8B57E45E

inbound esp sas:  
spi: 0x89898D1A(2307493146)  
transform: esp-3des esp-sha-hmac ,  
in use settings ={Tunnel, }  
slot: 0, conn id: 202, flow\_id: 3, crypto map: clientmap  
sa timing: remaining key lifetime (k/sec): (4607999/3452)  
IV size: 8 bytes  
replay detection support: Y

inbound ah sas:

inbound pcsp sas:

```
outbound esp sas:
spi: 0x8B57E45E(2337793118)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 203, flow_id: 4, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/3452)
IV size: 8 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
1710#show crypto engine connections active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
2	FastEthernet0	172.18.124.158	set	HMAC_SHA+3DES_56_C	0	0
200	FastEthernet0	172.18.124.158	set	HMAC_SHA+3DES_56_C	0	0
201	FastEthernet0	172.18.124.158	set	HMAC_SHA+3DES_56_C	0	0
202	FastEthernet0	172.18.124.158	set	HMAC_SHA+3DES_56_C	0	3
203	FastEthernet0	172.18.124.158	set	HMAC_SHA+3DES_56_C	3	0

## Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

### Команды для устранения неполадок

[Средство Output Interpreter \(OIT\) \(только для зарегистрированных клиентов\) поддерживает определенные команды show.](#) Используйте OIT для просмотра анализа выходных данных команды 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 — отображаются данные авторизации AAA/TACACS+.
- debug tacacs— показывает информацию, позволяющую найти и устранить неисправности в соединении между сервером TACACS+ и маршрутизатором.

### Журналы маршрутизатора

```
1710#show debug
General OS:
TACACS access control debugging is on
AAA Authentication debugging is on
AAA Authorization debugging is on
Cryptographic Subsystem:
Crypto ISAKMP debugging is on
Crypto Engine debugging is on
```



Crypto IPSEC debugging is on

1710#

**1w6d: ISAKMP (0:0): received packet from 192.168.60.34 (N) NEW SA**

1w6d: ISAKMP: local port 500, remote port 500

1w6d: ISAKMP (0:2): (Re)Setting client xauth list userauthen and state

1w6d: ISAKMP: Locking CONFIG struct 0x8158B894 from

crypto\_ikmp\_config\_initialize\_sa, count 2

1w6d: ISAKMP (0:2): processing SA payload. message ID = 0

1w6d: ISAKMP (0:2): processing ID payload. message ID = 0

1w6d: ISAKMP (0:2): processing vendor id payload

1w6d: ISAKMP (0:2): vendor ID seems Unity/DPD but bad major

1w6d: ISAKMP (0:2): vendor ID is XAUTH

1w6d: ISAKMP (0:2): processing vendor id payload

1w6d: ISAKMP (0:2): vendor ID is DPD

1w6d: ISAKMP (0:2): processing vendor id payload

1w6d: ISAKMP (0:2): vendor ID is Unity

1w6d: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 3 policy

1w6d: ISAKMP: encryption 3DES-CBC

1w6d: ISAKMP: hash SHA

1w6d: ISAKMP: default group 2

1w6d: ISAKMP: auth XAUTHInitPreShared

1w6d: ISAKMP: life type in seconds

1w6d: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B

**1w6d: ISAKMP (0:2): atts are acceptable. Next payload is 3**

1w6d: CryptoEngine0: generate alg parameter

1w6d: CryptoEngine0: CRYPTO\_ISA\_DH\_CREATE(hw)(ipsec)

1w6d: CRYPTO\_ENGINE: Dh phase 1 status: 0

1w6d: ISAKMP (0:2): processing KE payload. message ID = 0

1w6d: CryptoEngine0: generate alg parameter

1w6d: CryptoEngine0: CRYPTO\_ISA\_DH\_SHARE\_SECRET(hw)(ipsec)

1w6d: ISAKMP (0:2): processing NONCE payload. message ID = 0

1w6d: ISAKMP (0:2): processing vendor id payload

1w6d: ISAKMP (0:2): processing vendor id payload

1w6d: ISAKMP (0:2): processing vendor id payload

1w6d: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1

1w6d: AAA/MEMORY: create\_user (0x817F63F4) user='vpngroup' ruser='NULL' ds0=0

port='ISAKMP-ID-AUTH' rem\_addr='192.168.60.34' authen\_type=NONE

service=LOGIN priv=0 initial\_task\_id='0'

1w6d: ISAKMP (0:2): Input = IKE\_MSG\_FROM\_PEER, IKE\_AM\_EXCH

Old State = IKE\_READY New State = IKE\_R\_AM\_AAA\_AWAIT

1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894):

Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET

1w6d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(1472763894) user='vpngroup'

1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): send AV service=ike

1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): send AV protocol=ipsec

1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): found list "groupauthor"

1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): Method=LOCAL

1w6d: AAA/AUTHOR (1472763894): Post authorization status = PASS\_ADD

1w6d: ISAKMP: got callback 1

AAA/AUTHOR/IKE: Processing AV service=ike

AAA/AUTHOR/IKE: Processing AV protocol=ipsec

AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123

AAA/AUTHOR/IKE: Processing AV default-domain\*cisco.com

AAA/AUTHOR/IKE: Processing AV addr-pool\*ippool

AAA/AUTHOR/IKE: Processing AV key-exchange=ike

AAA/AUTHOR/IKE: Processing AV timeout\*0

AAA/AUTHOR/IKE: Processing AV idletime\*0

AAA/AUTHOR/IKE: Processing AV inacl\*102

AAA/AUTHOR/IKE: Processing AV dns-servers\*10.1.1.10 0.0.0.0

AAA/AUTHOR/IKE: Processing AV wins-servers\*10.1.1.20 0.0.0.0

1w6d: CryptoEngine0: create ISAKMP SKEYID for conn id 2

```
lw6d: CryptoEngine0: CRYPTO_ISA_SA_CREATE(hw)(ipsec)
lw6d: ISAKMP (0:2): SKEYID state generated
lw6d: ISAKMP (0:2): SA is doing pre-shared key authentication plus
    XAUTH using id type ID_IPV4_ADDR
lw6d: ISAKMP (2): ID payload
next-payload : 10
type : 1
protocol : 17
port : 500
length : 8
lw6d: ISAKMP (2): Total payload length: 12
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) AG_INIT_EXCH
lw6d: ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, PRESHARED_KEY_REPLY
Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

lw6d: AAA/MEMORY: free_user (0x817F63F4) user='vpngroup'
    ruser='NULL' port='ISAK MP-ID-AUTH' rem_addr='192.168.60.34'
    authen_type=NONE service=LOGIN priv=0
lw6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) AG_INIT_EXCH
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
lw6d: ISAKMP (0:2): processing HASH payload. message ID = 0
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: ISAKMP (0:2): processing NOTIFY INITIAL_CONTACT protocol 1
    spi 0, message ID = 0, sa = 81673884
lw6d: ISAKMP (0:2): Process initial contact, bring down
    existing phase 1 and 2 SA's
lw6d: ISAKMP (0:2): returning IP addr to the address pool: 10.1.1.113
lw6d: ISAKMP (0:2): returning address 10.1.1.113 to pool
lw6d: ISAKMP (0:2): peer does not do paranoid keepalives.

lw6d: ISAKMP (0:2): SA has been authenticated with 192.168.60.34
lw6d: CryptoEngine0: clear dh number for conn id 1
lw6d: CryptoEngine0: CRYPTO_ISA_DH_DELETE(hw)(ipsec)
lw6d: IPSEC(key_engine): got a queue event...
lw6d: IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
lw6d: IPSEC(key_engine_delete_sas): delete all SAs shared with 192.168.60.34
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
lw6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) QM_IDLE
lw6d: ISAKMP (0:2): purging node 1324880791
lw6d: ISAKMP: Sending phase 1 responder lifetime 86400

lw6d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

lw6d: ISAKMP (0:2): Need XAUTH
lw6d: AAA: parse name=ISAKMP idb type=-1 tty=-1
lw6d: AAA/MEMORY: create_user (0x812F79FC) user='NULL'
    ruser='NULL' ds0=0 port='
ISAKMP' rem_addr='192.168.60.34' authen_type=ASCII service=LOGIN
    priv=0 initial_task_id='0'
lw6d: ISAKMP (0:2): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT

lw6d: AAA/AUTHEN/START (2017610393): port='ISAKMP' list='userauthen'
    action=LOGIN service=LOGIN
lw6d: AAA/AUTHEN/START (2017610393): found list userauthen
lw6d: AAA/AUTHEN/START (2017610393): Method=tacacs+ (tacacs+)
lw6d: TAC+: send AUTHEN/START packet ver=192 id=2017610393
lw6d: TAC+: Using default tacacs server-group "tacacs+" list.
```

lw6d: TAC+: Opening TCP/IP to 172.16.124.96/49 timeout=5  
lw6d: TAC+: Opened TCP/IP handle 0x8183D638 to 172.16.124.96/49  
lw6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/START/LOGIN/ASCII queued  
lw6d: TAC+: (2017610393) AUTHEN/START/LOGIN/ASCII processed  
lw6d: TAC+: ver=192 id=2017610393 received AUTHEN status = GETUSER  
lw6d: AAA/AUTHEN(2017610393): Status=GETUSER  
lw6d: ISAKMP: got callback 1  
lw6d: ISAKMP/xauth: request attribute XAUTH\_TYPE\_V2  
lw6d: ISAKMP/xauth: request attribute XAUTH\_MESSAGE\_V2  
lw6d: ISAKMP/xauth: request attribute XAUTH\_USER\_NAME\_V2  
lw6d: ISAKMP/xauth: request attribute XAUTH\_USER\_PASSWORD\_V2  
lw6d: CryptoEngine0: generate hmac context for conn id 2  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec)  
lw6d: ISAKMP (0:2): initiating peer config to 192.168.60.34. ID = 1641488057  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_ENCRYPT(hw)(ipsec)  
lw6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF\_XAUTH  
lw6d: ISAKMP (0:2): Input = IKE\_MSG\_FROM\_AAA, IKE\_AAA\_START\_LOGIN  
Old State = IKE\_XAUTH\_AAA\_START\_LOGIN\_AWAIT  
New State = IKE\_XAUTH\_REQ\_SENT

lw6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) CONF\_XAUTH  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_DECRYPT(hw)(ipsec)  
lw6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.  
message ID = 1641488057  
lw6d: CryptoEngine0: generate hmac context for conn id 2  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec)  
lw6d: ISAKMP: Config payload REPLY  
lw6d: ISAKMP/xauth: reply attribute XAUTH\_TYPE\_V2 unexpected  
lw6d: ISAKMP/xauth: reply attribute XAUTH\_USER\_NAME\_V2  
lw6d: ISAKMP/xauth: reply attribute XAUTH\_USER\_PASSWORD\_V2  
lw6d: ISAKMP (0:2): deleting node 1641488057 error FALSE  
reason "done with xauth request/reply exchange"  
lw6d: ISAKMP (0:2): Input = IKE\_MSG\_FROM\_PEER, IKE\_CFG\_REPLY  
Old State = IKE\_XAUTH\_REQ\_SENT  
New State = IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT

lw6d: AAA/AUTHEN/CONT (2017610393): continue\_login (user='(undef)')  
lw6d: AAA/AUTHEN(2017610393): Status=GETUSER  
lw6d: AAA/AUTHEN(2017610393): Method=tacacs+ (tacacs+)  
lw6d: TAC+: send AUTHEN/CONT packet id=2017610393  
lw6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/CONT queued  
lw6d: TAC+: (2017610393) AUTHEN/CONT processed  
lw6d: TAC+: ver=192 id=2017610393 received AUTHEN status = GETPASS  
lw6d: AAA/AUTHEN(2017610393): Status=GETPASS  
lw6d: AAA/AUTHEN/CONT (2017610393): continue\_login (user='cisco')  
lw6d: AAA/AUTHEN(2017610393): Status=GETPASS  
lw6d: AAA/AUTHEN(2017610393): Method=tacacs+ (tacacs+)  
lw6d: TAC+: send AUTHEN/CONT packet id=2017610393  
lw6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/CONT queued  
lw6d: TAC+: (2017610393) AUTHEN/CONT processed  
lw6d: TAC+: ver=192 id=2017610393 received AUTHEN status = PASS  
lw6d: AAA/AUTHEN(2017610393): Status=PASS  
lw6d: ISAKMP: got callback 1  
lw6d: TAC+: Closing TCP/IP 0x8183D638 connection to 172.16.124.96/49  
lw6d: CryptoEngine0: generate hmac context for conn id 2  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec)  
lw6d: ISAKMP (0:2): initiating peer config to 192.168.60.34. ID = 1736579999  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_ENCRYPT(hw)(ipsec)  
lw6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF\_XAUTH  
lw6d: ISAKMP (0:2): Input = IKE\_MSG\_FROM\_AAA, IKE\_AAA\_CONT\_LOGIN  
Old State = IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT  
New State = IKE\_XAUTH\_SET\_SENT

lw6d: AAA/MEMORY: free\_user (0x812F79FC) user='cisco' ruser='NULL'

```
port='ISAKMP' rem_addr='192.168.60.34' authen_type=ASCII
service=LOGIN priv=0
lw6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) CONF_XAUTH
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
lw6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.
message ID = 1736579999
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: ISAKMP: Config payload ACK
lw6d: ISAKMP (0:2): XAUTH ACK Processed
lw6d: ISAKMP (0:2): deleting node 1736579999 error FALSE
reason "done with transaction"
lw6d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK
Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE

lw6d: ISAKMP (0:2): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

lw6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
lw6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.
message ID = 398811763
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: ISAKMP: Config payload REQUEST
lw6d: ISAKMP (0:2): checking request:
lw6d: ISAKMP: IP4_ADDRESS
lw6d: ISAKMP: IP4_NETMASK
lw6d: ISAKMP: IP4_DNS
lw6d: ISAKMP: IP4_NBNS
lw6d: ISAKMP: ADDRESS_EXPIRY
lw6d: ISAKMP: APPLICATION_VERSION
lw6d: ISAKMP: UNKNOWN Unknown Attr: 0x7000
lw6d: ISAKMP: UNKNOWN Unknown Attr: 0x7001
lw6d: ISAKMP: DEFAULT_DOMAIN
lw6d: ISAKMP: SPLIT_INCLUDE
lw6d: ISAKMP: UNKNOWN Unknown Attr: 0x7007
lw6d: ISAKMP: UNKNOWN Unknown Attr: 0x7008
lw6d: ISAKMP: UNKNOWN Unknown Attr: 0x7005
lw6d: AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1
lw6d: AAA/MEMORY: create_user (0x812F79FC) user='vpngroup' ruser='NULL' ds0=0 po
rt='ISAKMP-GROUP-AUTH' rem_addr='192.168.60.34' authen_type=NONE service=LOGIN pr
iv=0 initial_task_id='0'
lw6d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST
Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

lw6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET
lw6d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(1059453615)
user='vpngroup'
lw6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
send AV service=ike
lw6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
send AV protocol=ipsec
lw6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
found list "groupauthor"
lw6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
Method=LOCAL
lw6d: AAA/AUTHOR (1059453615): Post authorization status = PASS_ADD
lw6d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV service=ike
AAA/AUTHOR/IKE: Processing AV protocol=ipsec
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com
```

```
AAA/AUTHOR/IKE: Processing AV addr-pool*ippool
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV timeout*0
AAA/AUTHOR/IKE: Processing AV idletime*0
AAA/AUTHOR/IKE: Processing AV inacl*102
AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0
AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0
1w6d: ISAKMP (0:2): attributes sent in message:
1w6d: Address: 0.2.0.0
1w6d: ISAKMP (0:2): allocating address 10.1.1.114
1w6d: ISAKMP: Sending private address: 10.1.1.114
1w6d: ISAKMP: Unknown Attr: IP4_NETMASK (0x2)
1w6d: ISAKMP: Sending IP4_DNS server address: 10.1.1.10
1w6d: ISAKMP: Sending IP4_NBNS server address: 10.1.1.20
1w6d: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 86396
1w6d: ISAKMP: Sending APPLICATION_VERSION string:
Cisco Internetwork Operating System Software IOS (tm) C1700 Software
(C1710-K9O3SY-M), Version 12.2(8)T1, RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 30-Mar-02 13:30 by ccai
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7000)
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7001)
1w6d: ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com
1w6d: ISAKMP: Sending split include name 102 network 10.38.0.0
mask 255.255.0.0 protocol 0, src port 0, dst port 0

1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7007)
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7008)
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7005)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): responding to peer config from 192.168.60.34. ID = 398811763
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_ADDR
1w6d: ISAKMP (0:2): deleting node 398811763 error FALSE reason ""
1w6d: ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR
Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

1w6d: AAA/MEMORY: free_user (0x812F79FC) user='vpngroup'
ruser='NULL' port='ISAKMP-GROUP-AUTH' rem_addr='192.168.60.34'
authen_type=NONE service=LOGIN priv=0
1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): processing HASH payload. message ID = 1369459046
1w6d: ISAKMP (0:2): processing SA payload. message ID = 1369459046
1w6d: ISAKMP (0:2): Checking IPsec proposal 1
1w6d: ISAKMP: transform 1, ESP_3DES
1w6d: ISAKMP: attributes in transform:
1w6d: ISAKMP: authenticator is HMAC-MD5
1w6d: ISAKMP: encaps is 1
1w6d: ISAKMP: SA life type in seconds
1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: validate proposal 0
1w6d: IPSEC(validate_proposal): transform proposal
(proto 3, trans 3, hmac_alg 1) not supported
1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w6d: ISAKMP (0:2): skipping next ANDed proposal (1)
1w6d: ISAKMP (0:2): Checking IPsec proposal 2
1w6d: ISAKMP: transform 1, ESP_3DES
1w6d: ISAKMP: attributes in transform:
1w6d: ISAKMP: authenticator is HMAC-SHA
```

```
lw6d: ISAKMP: encaps is 1
lw6d: ISAKMP: SA life type in seconds
lw6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
lw6d: validate proposal 0
lw6d: ISAKMP (0:2): atts are acceptable.
lw6d: ISAKMP (0:2): Checking IPsec proposal 2
lw6d: ISAKMP (0:2): transform 1, IPPCP LZS
lw6d: ISAKMP: attributes in transform:
lw6d: ISAKMP: encaps is 1
lw6d: ISAKMP: SA life type in seconds
lw6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
lw6d: IPSEC(validate_proposal): transform proposal
    (prot 4, trans 3, hmac_alg 0) not supported
lw6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
lw6d: ISAKMP (0:2): Checking IPsec proposal 3
lw6d: ISAKMP: transform 1, ESP_3DES
lw6d: ISAKMP: attributes in transform:
lw6d: ISAKMP: authenticator is HMAC-MD5
lw6d: ISAKMP: encaps is 1
lw6d: ISAKMP: SA life type in seconds
lw6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
lw6d: validate proposal 0
lw6d: IPSEC(validate_proposal): transform proposal
    (prot 3, trans 3, hmac_alg 1) not supported
lw6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
lw6d: ISAKMP (0:2): Checking IPsec proposal 4
lw6d: ISAKMP: transform 1, ESP_3DES
lw6d: ISAKMP: attributes in transform:
lw6d: ISAKMP: authenticator is HMAC-SHA
lw6d: ISAKMP: encaps is 1
lw6d: ISAKMP: SA life type in seconds
lw6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
lw6d: validate proposal 0
lw6d: ISAKMP (0:2): atts are acceptable.
lw6d: IPSEC(validate_proposal_request): proposal part #1,
    (key eng. msg.) INBOUND local= 172.18.124.158,
    remote= 192.168.60.34, local_proxy= 172.18.124.158/255.255.255.255/0/0
    (type=1), remote_proxy= 10.1.1.114/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
lw6d: validate proposal request 0
lw6d: ISAKMP (0:2): processing NONCE payload. message ID = 1369459046
lw6d: ISAKMP (0:2): processing ID payload. message ID = 1369459046
lw6d: ISAKMP (0:2): processing ID payload. message ID = 1369459046
lw6d: ISAKMP (0:2): asking for 1 spis from ipsec
lw6d: ISAKMP (0:2): Node 1369459046, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE

lw6d: IPSEC(key_engine): got a queue event...
lw6d: IPSEC(spi_response): getting spi 1640315492 for SA
    from 172.18.124.158 to 192.168.60.34 for prot 3
lw6d: ISAKMP: received ke message (2/1)
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
lw6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) QM_IDLE
lw6d: ISAKMP (0:2): Node 1369459046,
    Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2

lw6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
```

```

lw6d: ipsec allocate flow 0
lw6d: ipsec allocate flow 0
lw6d: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)
lw6d: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)
lw6d: ISAKMP (0:2): Creating IPsec SAs
lw6d: inbound SA from 192.168.60.34 to 172.18.124.158
      (proxy 10.1.1.114 to 172.18.124.158)
lw6d: has spi 0x61C53A64 and conn_id 200 and flags 4
lw6d: lifetime of 2147483 seconds
lw6d: outbound SA from 172.18.124.158 to 192.168.60.34
      (proxy 172.18.124.158 to 10.1.1.114 )
lw6d: has spi -1885622177 and conn_id 201 and flags C
lw6d: lifetime of 2147483 seconds
lw6d: ISAKMP (0:2): deleting node 1369459046 error FALSE
      reason "quick mode done (await())"
lw6d: ISAKMP (0:2): Node 1369459046,
      Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

lw6d: IPSEC(key_engine): got a queue event...
lw6d: IPSEC(initialize_sas): ,
      (key eng. msg.) INBOUND local= 172.18.124.158,
      remote= 192.168.60.34, local_proxy= 172.18.124.158/0.0.0.0/0/0
      (type=1), remote_proxy= 10.1.1.114/0.0.0.0/0/0 (type=1),
      protocol= ESP, transform= esp-3des esp-sha-hmac ,
      lifedur= 2147483s and 0kb, spi= 0x61C53A64(1640315492),
      conn_id= 200, keysize= 0, flags= 0x4
lw6d: IPSEC(initialize_sas): , (key eng. msg.)
      OUTBOUND local= 172.18.124.158, remote= 192.168.60.34,
      local_proxy= 172.18.124.158/0.0.0.0/0/0 (type=1),
      remote_proxy= 10.1.1.114/0.0.0.0/0/0 (type=1),
      protocol= ESP, transform= esp-3des esp-sha-hmac ,
      lifedur= 2147483s and 0kb, spi= 0x8F9BB05F(2409345119),
      conn_id= 201, keysize= 0, flags= 0xC
lw6d: IPSEC(create_sa): sa created, (sa) sa_dest= 172.18.124.158,
      sa_prot= 50, sa_spi= 0x61C53A64(1640315492),
      sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 200
lw6d: IPSEC(create_sa): sa created, (sa) sa_dest= 192.168.60.34,
      sa_prot= 50, sa_spi= 0x8F9BB05F(2409345119),
      sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 201

```

## [Журналы клиента](#)

*Для просмотра журналов запустите средство Log Viewer на клиенте VPN и задайте для всех настроенных классов уровень фильтра High (высокий).*

Пример выходной информации в журнале показан здесь.

```

1710#show debug
General OS:
TACACS access control debugging is on
AAA Authentication debugging is on
AAA Authorization debugging is on
Cryptographic Subsystem:
Crypto ISAKMP debugging is on
Crypto Engine debugging is on
Crypto IPSEC debugging is on

1710#
lw6d: ISAKMP (0:0): received packet from 192.168.60.34 (N) NEW SA
lw6d: ISAKMP: local port 500, remote port 500
lw6d: ISAKMP (0:2): (Re)Setting client xauth list userauthen and state

```

```
1w6d: ISAKMP: Locking CONFIG struct 0x8158B894 from
    crypto_ikmp_config_initialize_sa, count 2
1w6d: ISAKMP (0:2): processing SA payload. message ID = 0
1w6d: ISAKMP (0:2): processing ID payload. message ID = 0
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): vendor ID seems Unity/DPD but bad major
1w6d: ISAKMP (0:2): vendor ID is XAUTH
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): vendor ID is DPD
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): vendor ID is Unity
1w6d: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 3 policy
1w6d: ISAKMP: encryption 3DES-CBC
1w6d: ISAKMP: hash SHA
1w6d: ISAKMP: default group 2
1w6d: ISAKMP: auth XAUTHInitPreShared
1w6d: ISAKMP: life type in seconds
1w6d: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: ISAKMP (0:2): atts are acceptable. Next payload is 3
1w6d: CryptoEngine0: generate alg parameter
1w6d: CryptoEngine0: CRYPTO_ISA_DH_CREATE(hw)(ipsec)
1w6d: CRYPTO_ENGINE: Dh phase 1 status: 0
1w6d: ISAKMP (0:2): processing KE payload. message ID = 0
1w6d: CryptoEngine0: generate alg parameter
1w6d: CryptoEngine0: CRYPTO_ISA_DH_SHARE_SECRET(hw)(ipsec)
1w6d: ISAKMP (0:2): processing NONCE payload. message ID = 0
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1
1w6d: AAA/MEMORY: create_user (0x817F63F4) user='vpngroup' ruser='NULL' ds0=0
    port='ISAKMP-ID-AUTH' rem_addr='192.168.60.34' authen_type=NONE
    service=LOGIN priv=0 initial_task_id='0'
1w6d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT

1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894):
    Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET
1w6d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(1472763894) user='vpngroup'
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): send AV service=ike
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): send AV protocol=ipsec
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): found list "groupauthor"
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): Method=LOCAL
1w6d: AAA/AUTHOR (1472763894): Post authorization status = PASS_ADD
1w6d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV service=ike
AAA/AUTHOR/IKE: Processing AV protocol=ipsec
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com
AAA/AUTHOR/IKE: Processing AV addr-pool*ippool
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV timeout*0
AAA/AUTHOR/IKE: Processing AV idletime*0
AAA/AUTHOR/IKE: Processing AV inacl*102
AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0
AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0
1w6d: CryptoEngine0: create ISAKMP SKEYID for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_SA_CREATE(hw)(ipsec)
1w6d: ISAKMP (0:2): SKEYID state generated
1w6d: ISAKMP (0:2): SA is doing pre-shared key authentication plux
    XAUTH using id type ID_IPV4_ADDR
1w6d: ISAKMP (2): ID payload
next-payload : 10
type : 1
```



```
protocol : 17
port : 500
length : 8
lw6d: ISAKMP (2): Total payload length: 12
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) AG_INIT_EXCH
lw6d: ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, PRESHARED_KEY_REPLY
Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

lw6d: AAA/MEMORY: free_user (0x817F63F4) user='vpngroup'
      ruser='NULL' port='ISAK MP-ID-AUTH' rem_addr='192.168.60.34'
      authen_type=NONE service=LOGIN priv=0
lw6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) AG_INIT_EXCH
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
lw6d: ISAKMP (0:2): processing HASH payload. message ID = 0
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: ISAKMP (0:2): processing NOTIFY INITIAL_CONTACT protocol 1
      spi 0, message ID = 0, sa = 81673884
lw6d: ISAKMP (0:2): Process initial contact, bring down
      existing phase 1 and 2 SA's
lw6d: ISAKMP (0:2): returning IP addr to the address pool: 10.1.1.113
lw6d: ISAKMP (0:2): returning address 10.1.1.113 to pool
lw6d: ISAKMP (0:2): peer does not do paranoid keepalives.

lw6d: ISAKMP (0:2): SA has been authenticated with 192.168.60.34
lw6d: CryptoEngine0: clear dh number for conn id 1
lw6d: CryptoEngine0: CRYPTO_ISA_DH_DELETE(hw)(ipsec)
lw6d: IPSEC(key_engine): got a queue event...
lw6d: IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
lw6d: IPSEC(key_engine_delete_sas): delete all SAs shared with 192.168.60.34
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
lw6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) QM_IDLE
lw6d: ISAKMP (0:2): purging node 1324880791
lw6d: ISAKMP: Sending phase 1 responder lifetime 86400

lw6d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

lw6d: ISAKMP (0:2): Need XAUTH
lw6d: AAA: parse name=ISAKMP idb type=-1 tty=-1
lw6d: AAA/MEMORY: create_user (0x812F79FC) user='NULL'
      ruser='NULL' ds0=0 port='
ISAKMP' rem_addr='192.168.60.34' authen_type=ASCII service=LOGIN
      priv=0 initial_task_id='0'
lw6d: ISAKMP (0:2): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT

lw6d: AAA/AUTHEN/START (2017610393): port='ISAKMP' list='userauthen'
      action=LOGIN service=LOGIN
lw6d: AAA/AUTHEN/START (2017610393): found list userauthen
lw6d: AAA/AUTHEN/START (2017610393): Method=tacacs+ (tacacs+)
lw6d: TAC+: send AUTHEN/START packet ver=192 id=2017610393
lw6d: TAC+: Using default tacacs server-group "tacacs+" list.
lw6d: TAC+: Opening TCP/IP to 172.16.124.96/49 timeout=5
lw6d: TAC+: Opened TCP/IP handle 0x8183D638 to 172.16.124.96/49
lw6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/START/LOGIN/ASCII queued
lw6d: TAC+: (2017610393) AUTHEN/START/LOGIN/ASCII processed
lw6d: TAC+: ver=192 id=2017610393 received AUTHEN status = GETUSER
lw6d: AAA/AUTHEN(2017610393): Status=GETUSER
lw6d: ISAKMP: got callback 1
```

lw6d: ISAKMP/xauth: request attribute XAUTH\_TYPE\_V2  
lw6d: ISAKMP/xauth: request attribute XAUTH\_MESSAGE\_V2  
lw6d: ISAKMP/xauth: request attribute XAUTH\_USER\_NAME\_V2  
lw6d: ISAKMP/xauth: request attribute XAUTH\_USER\_PASSWORD\_V2  
lw6d: CryptoEngine0: generate hmac context for conn id 2  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec)  
lw6d: ISAKMP (0:2): initiating peer config to 192.168.60.34. ID = 1641488057  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_ENCRYPT(hw)(ipsec)  
lw6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF\_XAUTH  
lw6d: ISAKMP (0:2): Input = IKE\_MSG\_FROM\_AAA, IKE\_AAA\_START\_LOGIN  
Old State = IKE\_XAUTH\_AAA\_START\_LOGIN\_AWAIT  
New State = IKE\_XAUTH\_REQ\_SENT

lw6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) CONF\_XAUTH  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_DECRYPT(hw)(ipsec)  
lw6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.  
message ID = 1641488057  
lw6d: CryptoEngine0: generate hmac context for conn id 2  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec)  
lw6d: ISAKMP: Config payload REPLY  
lw6d: ISAKMP/xauth: reply attribute XAUTH\_TYPE\_V2 unexpected  
lw6d: ISAKMP/xauth: reply attribute XAUTH\_USER\_NAME\_V2  
lw6d: ISAKMP/xauth: reply attribute XAUTH\_USER\_PASSWORD\_V2  
lw6d: ISAKMP (0:2): deleting node 1641488057 error FALSE  
reason "done with xauth request/reply exchange"  
lw6d: ISAKMP (0:2): Input = IKE\_MSG\_FROM\_PEER, IKE\_CFG\_REPLY  
Old State = IKE\_XAUTH\_REQ\_SENT  
New State = IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT

lw6d: AAA/AUTHEN/CONT (2017610393): continue\_login (user='(undef)')  
lw6d: AAA/AUTHEN(2017610393): Status=GETUSER  
lw6d: AAA/AUTHEN(2017610393): Method=tacacs+ (tacacs+)  
lw6d: TAC+: send AUTHEN/CONT packet id=2017610393  
lw6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/CONT queued  
lw6d: TAC+: (2017610393) AUTHEN/CONT processed  
**lw6d: TAC+: ver=192 id=2017610393 received AUTHEN status = GETPASS**  
lw6d: AAA/AUTHEN(2017610393): Status=GETPASS  
lw6d: AAA/AUTHEN/CONT (2017610393): continue\_login (user='cisco')  
lw6d: AAA/AUTHEN(2017610393): Status=GETPASS  
lw6d: AAA/AUTHEN(2017610393): Method=tacacs+ (tacacs+)  
lw6d: TAC+: send AUTHEN/CONT packet id=2017610393  
lw6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/CONT queued  
lw6d: TAC+: (2017610393) AUTHEN/CONT processed  
**lw6d: TAC+: ver=192 id=2017610393 received AUTHEN status = PASS**  
lw6d: AAA/AUTHEN(2017610393): Status=PASS  
lw6d: ISAKMP: got callback 1  
lw6d: TAC+: Closing TCP/IP 0x8183D638 connection to 172.16.124.96/49  
lw6d: CryptoEngine0: generate hmac context for conn id 2  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec)  
lw6d: ISAKMP (0:2): initiating peer config to 192.168.60.34. ID = 1736579999  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_ENCRYPT(hw)(ipsec)  
lw6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF\_XAUTH  
lw6d: ISAKMP (0:2): Input = IKE\_MSG\_FROM\_AAA, IKE\_AAA\_CONT\_LOGIN  
Old State = IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT  
New State = IKE\_XAUTH\_SET\_SENT

lw6d: AAA/MEMORY: free\_user (0x812F79FC) user='cisco' ruser='NULL'  
port='ISAKMP' rem\_addr='192.168.60.34' authen\_type=ASCII  
service=LOGIN priv=0  
lw6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) CONF\_XAUTH  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_DECRYPT(hw)(ipsec)  
lw6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.  
message ID = 1736579999  
lw6d: CryptoEngine0: generate hmac context for conn id 2

```
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: ISAKMP: Config payload ACK
lw6d: ISAKMP (0:2): XAUTH ACK Processed
lw6d: ISAKMP (0:2): deleting node 1736579999 error FALSE
    reason "done with transaction"
lw6d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK
Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE

lw6d: ISAKMP (0:2): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

lw6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
lw6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.
    message ID = 398811763
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: ISAKMP: Config payload REQUEST
lw6d: ISAKMP (0:2): checking request:
lw6d: ISAKMP: IP4_ADDRESS
lw6d: ISAKMP: IP4_NETMASK
lw6d: ISAKMP: IP4_DNS
lw6d: ISAKMP: IP4_NBNS
lw6d: ISAKMP: ADDRESS_EXPIRY
lw6d: ISAKMP: APPLICATION_VERSION
lw6d: ISAKMP: UNKNOWN Unknown Attr: 0x7000
lw6d: ISAKMP: UNKNOWN Unknown Attr: 0x7001
lw6d: ISAKMP: DEFAULT_DOMAIN
lw6d: ISAKMP: SPLIT_INCLUDE
lw6d: ISAKMP: UNKNOWN Unknown Attr: 0x7007
lw6d: ISAKMP: UNKNOWN Unknown Attr: 0x7008
lw6d: ISAKMP: UNKNOWN Unknown Attr: 0x7005
lw6d: AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1
lw6d: AAA/MEMORY: create_user (0x812F79FC) user='vpngroup' ruser='NULL' ds0=0 po
rt='ISAKMP-GROUP-AUTH' rem_addr='192.168.60.34' authen_type=NONE service=LOGIN pr
iv=0 initial_task_id='0'
lw6d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST
Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

lw6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
    Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET
lw6d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(1059453615)
    user='vpngroup'
lw6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
    send AV service=ike
lw6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
    send AV protocol=ipsec
lw6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
    found list "groupauthor"
lw6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
    Method=LOCAL
lw6d: AAA/AUTHOR (1059453615): Post authorization status = PASS_ADD
lw6d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV service=ike
AAA/AUTHOR/IKE: Processing AV protocol=ipsec
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com
AAA/AUTHOR/IKE: Processing AV addr-pool*ippool
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV timeout*0
AAA/AUTHOR/IKE: Processing AV idletime*0
AAA/AUTHOR/IKE: Processing AV inacl*102
AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0
AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0
```

```
lw6d: ISAKMP (0:2): attributes sent in message:
lw6d: Address: 0.2.0.0
lw6d: ISAKMP (0:2): allocating address 10.1.1.114
lw6d: ISAKMP: Sending private address: 10.1.1.114
lw6d: ISAKMP: Unknown Attr: IP4_NETMASK (0x2)
lw6d: ISAKMP: Sending IP4_DNS server address: 10.1.1.10
lw6d: ISAKMP: Sending IP4_NBNS server address: 10.1.1.20
lw6d: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 86396
lw6d: ISAKMP: Sending APPLICATION_VERSION string:
Cisco Internetwork Operating System Software IOS (tm) C1700 Software
(C1710-K9O3SY-M), Version 12.2(8)T1, RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 30-Mar-02 13:30 by ccai
lw6d: ISAKMP: Unknown Attr: UNKNOWN (0x7000)
lw6d: ISAKMP: Unknown Attr: UNKNOWN (0x7001)
lw6d: ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com
lw6d: ISAKMP: Sending split include name 102 network 10.38.0.0
mask 255.255.0.0 protocol 0, src port 0, dst port 0

lw6d: ISAKMP: Unknown Attr: UNKNOWN (0x7007)
lw6d: ISAKMP: Unknown Attr: UNKNOWN (0x7008)
lw6d: ISAKMP: Unknown Attr: UNKNOWN (0x7005)
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: ISAKMP (0:2): responding to peer config from 192.168.60.34. ID = 398811763
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
lw6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_ADDR
lw6d: ISAKMP (0:2): deleting node 398811763 error FALSE reason ""
lw6d: ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR
Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

lw6d: AAA/MEMORY: free_user (0x812F79FC) user='vpngroup'
ruser='NULL' port='ISAKMP-GROUP-AUTH' rem_addr='192.168.60.34'
authen_type=NONE service=LOGIN priv=0
lw6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
lw6d: CryptoEngine0: generate hmac context for conn id 2
lw6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
lw6d: ISAKMP (0:2): processing HASH payload. message ID = 1369459046
lw6d: ISAKMP (0:2): processing SA payload. message ID = 1369459046
lw6d: ISAKMP (0:2): Checking IPsec proposal 1
lw6d: ISAKMP: transform 1, ESP_3DES
lw6d: ISAKMP: attributes in transform:
lw6d: ISAKMP: authenticator is HMAC-MD5
lw6d: ISAKMP: encaps is 1
lw6d: ISAKMP: SA life type in seconds
lw6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
lw6d: validate proposal 0
lw6d: IPSEC(validate_proposal): transform proposal
(proto 3, trans 3, hmac_alg 1) not supported
lw6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
lw6d: ISAKMP (0:2): skipping next ANDed proposal (1)
lw6d: ISAKMP (0:2): Checking IPsec proposal 2
lw6d: ISAKMP: transform 1, ESP_3DES
lw6d: ISAKMP: attributes in transform:
lw6d: ISAKMP: authenticator is HMAC-SHA
lw6d: ISAKMP: encaps is 1
lw6d: ISAKMP: SA life type in seconds
lw6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
lw6d: validate proposal 0
lw6d: ISAKMP (0:2): atts are acceptable.
lw6d: ISAKMP (0:2): Checking IPsec proposal 2
lw6d: ISAKMP (0:2): transform 1, IPPCP LZS
```

lw6d: ISAKMP: attributes in transform:  
lw6d: ISAKMP: encaps is 1  
lw6d: ISAKMP: SA life type in seconds  
lw6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
lw6d: IPSEC(validate\_proposal): transform proposal  
    (prot 4, trans 3, hmac\_alg 0) not supported  
lw6d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
lw6d: ISAKMP (0:2): Checking IPsec proposal 3  
lw6d: ISAKMP: transform 1, ESP\_3DES  
lw6d: ISAKMP: attributes in transform:  
lw6d: ISAKMP: authenticator is HMAC-MD5  
lw6d: ISAKMP: encaps is 1  
lw6d: ISAKMP: SA life type in seconds  
lw6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
lw6d: validate proposal 0  
lw6d: IPSEC(validate\_proposal): transform proposal  
    (prot 3, trans 3, hmac\_alg 1) not supported  
lw6d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
lw6d: ISAKMP (0:2): Checking IPsec proposal 4  
lw6d: ISAKMP: transform 1, ESP\_3DES  
lw6d: ISAKMP: attributes in transform:  
lw6d: ISAKMP: authenticator is HMAC-SHA  
lw6d: ISAKMP: encaps is 1  
lw6d: ISAKMP: SA life type in seconds  
lw6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
lw6d: validate proposal 0  
**lw6d: ISAKMP (0:2): atts are acceptable.**  
lw6d: IPSEC(validate\_proposal\_request): proposal part #1,  
    (key eng. msg.) INBOUND local= 172.18.124.158,  
    remote= 192.168.60.34, local\_proxy= 172.18.124.158/255.255.255.255/0/0  
    (type=1), remote\_proxy= 10.1.1.114/255.255.255.255/0/0 (type=1),  
    protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 0s and 0kb,  
    spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4  
lw6d: validate proposal request 0  
lw6d: ISAKMP (0:2): processing NONCE payload. message ID = 1369459046  
lw6d: ISAKMP (0:2): processing ID payload. message ID = 1369459046  
lw6d: ISAKMP (0:2): processing ID payload. message ID = 1369459046  
lw6d: ISAKMP (0:2): asking for 1 spis from ipsec  
lw6d: ISAKMP (0:2): Node 1369459046, Input = IKE\_MSG\_FROM\_PEER, IKE\_QM\_EXCH  
Old State = IKE\_QM\_READY New State = IKE\_QM\_SPI\_STARVE  
  
lw6d: IPSEC(key\_engine): got a queue event...  
lw6d: IPSEC(spi\_response): getting spi 1640315492 for SA  
    from 172.18.124.158 to 192.168.60.34 for prot 3  
lw6d: ISAKMP: received ke message (2/1)  
lw6d: CryptoEngine0: generate hmac context for conn id 2  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec)  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_ENCRYPT(hw)(ipsec)  
lw6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) QM\_IDLE  
lw6d: ISAKMP (0:2): Node 1369459046,  
    Input = IKE\_MSG\_FROM\_IPSEC, IKE\_SPI\_REPLY  
Old State = IKE\_QM\_SPI\_STARVE New State = IKE\_QM\_R\_QM2  
  
lw6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM\_IDLE  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_DECRYPT(hw)(ipsec)  
lw6d: CryptoEngine0: generate hmac context for conn id 2  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IKE\_HMAC(hw)(ipsec)  
lw6d: ipsec allocate flow 0  
lw6d: ipsec allocate flow 0  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IPSEC\_KEY\_CREATE(hw)(ipsec)  
lw6d: CryptoEngine0: CRYPTO\_ISA\_IPSEC\_KEY\_CREATE(hw)(ipsec)  
lw6d: ISAKMP (0:2): Creating IPsec SAs  
lw6d: inbound SA from 192.168.60.34 to 172.18.124.158  
    (proxy 10.1.1.114 to 172.18.124.158)

```
lw6d: has spi 0x61C53A64 and conn_id 200 and flags 4
lw6d: lifetime of 2147483 seconds
lw6d: outbound SA from 172.18.124.158 to 192.168.60.34
      (proxy 172.18.124.158 to 10.1.1.114 )
lw6d: has spi -1885622177 and conn_id 201 and flags C
lw6d: lifetime of 2147483 seconds
lw6d: ISAKMP (0:2): deleting node 1369459046 error FALSE
      reason "quick mode done (await())"
lw6d: ISAKMP (0:2): Node 1369459046,
      Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

lw6d: IPSEC(key_engine): got a queue event...
lw6d: IPSEC(initialize_sas): ,
      (key eng. msg.) INBOUND local= 172.18.124.158,
      remote= 192.168.60.34, local_proxy= 172.18.124.158/0.0.0.0/0/0
      (type=1), remote_proxy= 10.1.1.114/0.0.0.0/0/0 (type=1),
      protocol= ESP, transform= esp-3des esp-sha-hmac ,
      lifedur= 2147483s and 0kb, spi= 0x61C53A64(1640315492),
      conn_id= 200, keysize= 0, flags= 0x4
lw6d: IPSEC(initialize_sas): , (key eng. msg.)
      OUTBOUND local= 172.18.124.158, remote= 192.168.60.34,
      local_proxy= 172.18.124.158/0.0.0.0/0/0 (type=1),
      remote_proxy= 10.1.1.114/0.0.0.0/0/0 (type=1),
      protocol= ESP, transform= esp-3des esp-sha-hmac ,
      lifedur= 2147483s and 0kb, spi= 0x8F9BB05F(2409345119),
      conn_id= 201, keysize= 0, flags= 0xC
lw6d: IPSEC(create_sa): sa created, (sa) sa_dest= 172.18.124.158,
      sa_prot= 50, sa_spi= 0x61C53A64(1640315492),
      sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 200
lw6d: IPSEC(create_sa): sa created, (sa) sa_dest= 192.168.60.34,
      sa_prot= 50, sa_spi= 0x8F9BB05F(2409345119),
      sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 201
```

## Дополнительные сведения

- [Поддержка системы управления доступом на основе контроллера терминального доступа \(TACACS+\)](#)
- [Поддержка сервера Cisco Secure Access Control Server для Unix](#)
- [Поддержка Cisco Secure ACS для Windows](#)
- [Поддержка клиента Cisco VPN Client](#)
- [Страница поддержки IPsec Negotiation/IKE](#)
- [Cisco Systems – техническая поддержка и документация](#)