

Настройка общих ключей IKE с помощью сервера RADIUS для клиента Cisco Secure VPN Client

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Создание профиля Cisco Secure](#)

[Выбор конфигурации маршрутизатора](#)

[Настройка клиента](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

Введение

В настоящем документе описано, как конфигурировать совместно используемый секретный пароль обмена ключами в Internet (IKE) при помощи сервера службы удаленной аутентификации по телефону. Функция общего секрета IKE, которая использует аутентификацию, авторизацию и учет (AAA), включает ключевой поиск от AAA-сервера. Предварительные общие ключи не масштабируются хорошо при развертывании крупномасштабной системы VPN без центра сертификации (CA). При использовании динамического IP, обращаясь, такого как Протокол DHCP (динамического конфигурирования узла) или модемные связи Протокола PPP, изменяющийся IP-адрес может сделать ключевой поиск трудным или невозможным, пока не используется предварительный общий ключ подстановочного знака. В совместно используемой IKE секретной функции, которая использует AAA сервер, доступ к общему секрету получается в агрессивном режиме согласования IKE через сервер AAA. Идентификатор обмена используется в качестве имени пользователя для отправки запроса AAA, если не найден локальный ключ маршрутизатора Cisco IOS®, к которому пользователь пытается подключиться. Это было представлено в программном обеспечении Cisco IOS версии 12.1. T. Для использования этого средства необходим включенный агрессивный режим на клиенте VPN.

Предварительные условия

Требования

Необходимо было включить агрессивный режим на Клиенте VPN, и необходимо выполнять программное обеспечение Cisco IOS версии 12.1. T или позже маршрутизатор.

Используемые компоненты

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

- Cisco Secure ACS для Windows
- Cisco IOS Software Release 12.2.8T
- Маршрутизатор Cisco 1700

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

[Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.](#)

Настройка

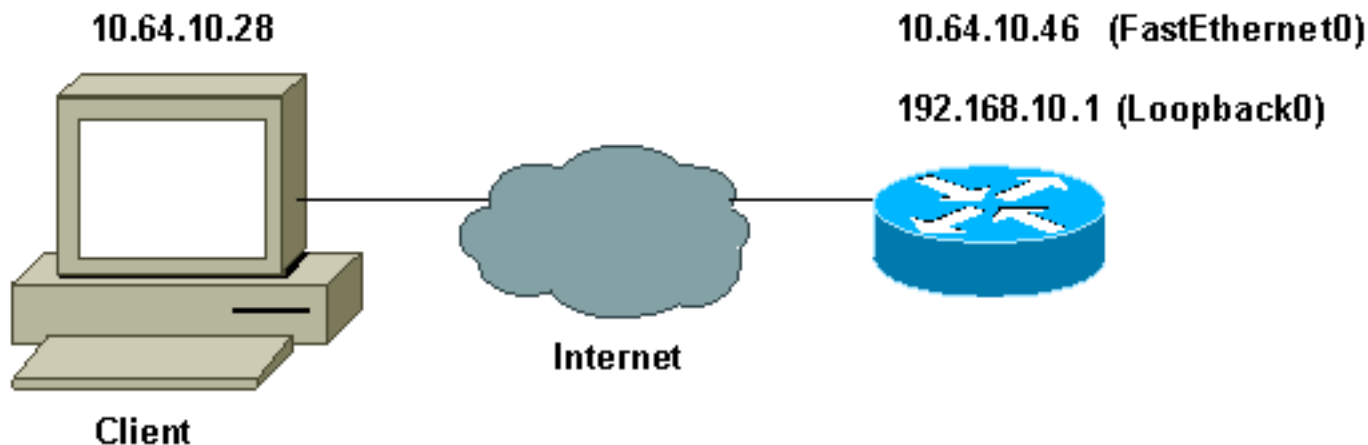
В данном документе используются следующие конфигурации.

- [Создание профиля Cisco Secure](#)
- [Выбор конфигурации маршрутизатора](#)
- [Настройка клиента](#)

Примечание: [Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" \(Поиск команд\) \(только для зарегистрированных клиентов\).](#)

Схема сети

В настоящем документе используется следующая схема сети:



Создание профиля Cisco Secure

Этот профиль был создан с UNIX, но подобный профиль может быть создан на Cisco Secure ACS для Windows.

```
# ./ViewProfile -p 9900 -u haseeb
User Profile Information
!--- The user name is sent by the VPN Client; !--- look at the client configuration. user =
haseeb{

radius=Cisco12.05 {
check_items= {
!--- This should always be "cisco." 2=cisco
}
reply_attributes= {
6=5
64=9
65=1
!--- Pre-shared key. 9,1="ipsec:tunnel-password=secret12345"
9,1="ipsec:key-exchange=ike"
}
}
}
```

Эти выходные данные показывают сценарий, который используется для добавления профиля пользователя в Cisco Secure ACS для UNIX.

```
# ./ViewProfile -p 9900 -u haseeb
User Profile Information
!--- The user name is sent by the VPN Client; !--- look at the client configuration. user =
haseeb{

radius=Cisco12.05 {
check_items= {
!--- This should always be "cisco." 2=cisco
}
reply_attributes= {
6=5
64=9
65=1
!--- Pre-shared key. 9,1="ipsec:tunnel-password=secret12345"
9,1="ipsec:key-exchange=ike"
}
}
}
```

Выполните эти действия для использования GUI для настройки профиля пользователя на Cisco Secure ACS для Windows 2.6.

1. Определите имя пользователя, используйте слово cisco в качестве

The screenshot shows the 'Edit' page for a user named 'haseeb'. It includes a checkbox for 'Account Disabled', a 'Supplementary User Info' section with fields for 'Real Name' (haseeb) and 'Description' (vpn user), and a 'User Setup' section. The 'User Setup' section has a 'Password Authentication' dropdown set to 'CiscoSecure Database' and two password fields labeled 'Password' and 'Confirm Password', both containing masked characters.

пароля.

2. Определите обмен ключами как IKE и предварительно распределенный ключ в Cisco

The screenshot shows the 'Cisco IOS/PIX RADIUS Attributes' configuration page. A checkbox is checked for '[009\001] cisco-av-pair'. Below this, a text area contains the configuration commands: 'ipsec:tunnel-', 'password=secret12345', and 'ipsec:key-exchange=ike'.

av-pair.

[Выбор конфигурации маршрутизатора](#)

Cisco 1751 с IOS 12.2.8T

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```

!
hostname 1751-vpn
!
!--- Enable AAA. aaa new-model
!
!
aaa authentication login default none
!--- Configure authorization. aaa authorization network
vpn_users group radius
aaa session-id common
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
no ip domain-lookup
!
!--- Define IKE policy for phase 1 negotiations of the
VPN Clients. crypto isakmp policy 10
  hash md5
  authentication pre-share
crypto isakmp client configuration address-pool local
mypool
!
!--- Define IPSec policies - Phase 2 Policy for actual
data encryption. crypto ipsec transform-set myset esp-
des esp-md5-hmac
!
!--- Create dynamic crypto map. crypto dynamic-map
dynmap 10
  set transform-set myset
!
!--- Configure IKE shared secret using AAA server on
this router. crypto map intmap isakmp authorization list
vpn_users
!--- IKE Mode Configuration - the router will attempt !-
-- to set IP addresses for each peer. crypto map intmap
client configuration address initiate
!--- IKE Mode Configuration - the router will accept !--
- requests for IP addresses from any requesting peer.
crypto map intmap client configuration address respond
crypto map intmap 10 ipsec-isakmp dynamic dynmap
!
interface Loopback0
  ip address 192.168.10.1 255.255.255.0
!
interface Loopback1
  no ip address
!
interface Ethernet0/0
  no ip address
  half-duplex
!
interface FastEthernet0/0
  ip address 10.64.10.46 255.255.255.224
  speed auto
!--- Assign crypto map to interface. crypto map intmap
!
!--- Configure a local pool of IP addresses to be used
when a !--- remote peer connects to a point-to-point
interface. ip local pool mypool 10.1.2.1 10.1.2.254

```

```

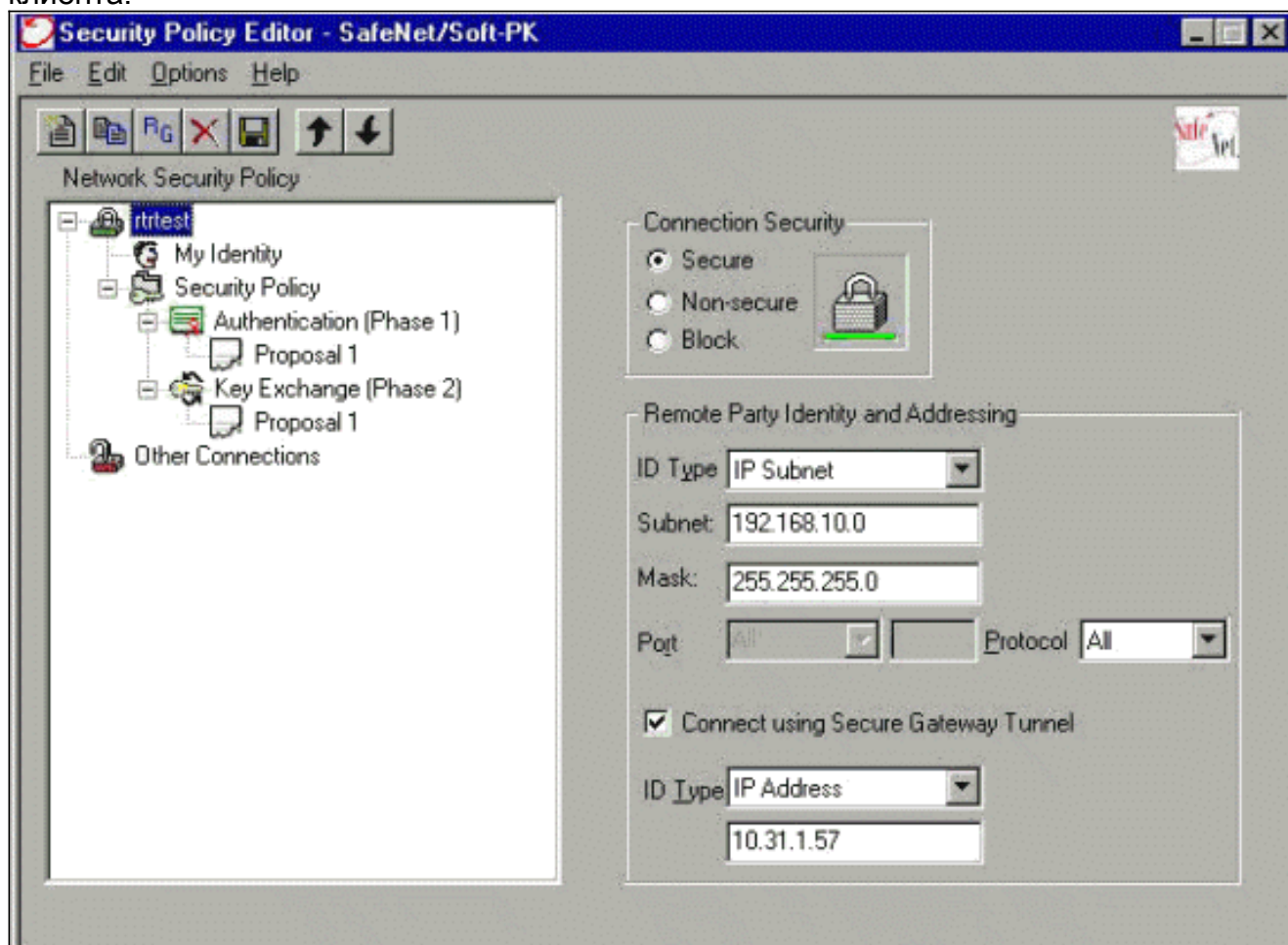
ip classless
ip route 0.0.0.0 0.0.0.0 10.64.10.33
no ip http server
ip pim bidir-enable
!
!--- Specify the security server protocol and defines
security !--- server host IP address and UDP port
number. radius-server host 10.64.10.7 auth-port 1645
acct-port 1646 key cisco123
radius-server retransmit 3
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
!
end

```

Настройка клиента

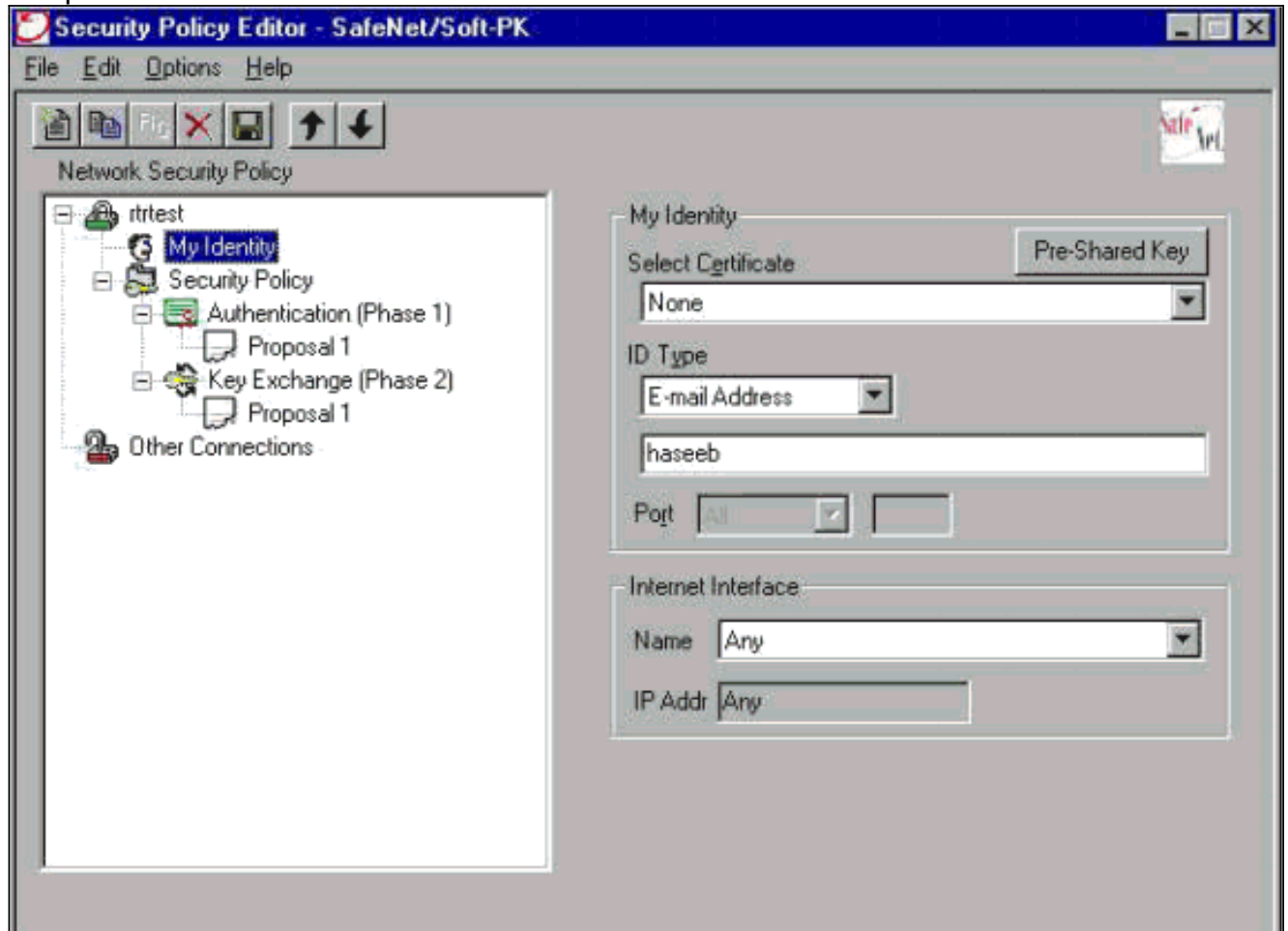
Выполните эти действия для настройки клиента.

1. В Редакторе Политики безопасности перейдите к **Network Security Policy> rtrtest**. Выберите **ID Type** как адрес электронной почты и вставьте имя пользователя, которое будет настроено на сервере RADIUS. Если для этого параметра оставить значение IP Address, то имя пользователя, отправляемое серверу RADIUS, будет IP-адресом компьютера клиента.



2. Перейдите к **Network Security Policy> rtrtest> My Identity** и выберите **Aggressive Mode**.

Настройка не будет работать, если данный режим не выбран.



Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Эти выходные данные показывают хорошие отладки для этой конфигурации:

```
23:43:41: ISAKMP (0:0): received packet from 10.64.10.28 (N) NEW SA
23:43:41: ISAKMP: local port 500, remote port 500
23:43:41: ISAKMP: Locking CONFIG struct 0x8180BEF4 from
crypto_ikmp_config_initialize_sa, count 2
23:43:41: ISAKMP (0:3): processing SA payload. message ID = 0
23:43:41: ISAKMP (0:3): processing ID payload. message ID = 0
23:43:41: ISAKMP (0:3): processing vendor id payload
23:43:41: ISAKMP (0:3): vendor ID seems Unity/DPD but bad major
23:43:41: ISAKMP (0:3): vendor ID is XAUTH
23:43:41: ISAKMP (0:3): Checking ISAKMP transform 1 against priority 10 policy
23:43:41: ISAKMP: encryption DES-CBC
23:43:41: ISAKMP: hash MD5
23:43:41: ISAKMP: default group 1
23:43:41: ISAKMP: auth pre-share
!--- ISAKMP policy proposed by VPN Client !--- matched the configured ISAKMP policy. 23:43:41:
```

```
ISAKMP (0:3): atts are acceptable. Next payload is 0
23:43:41: ISAKMP (0:3): processing KE payload. message ID = 0
23:43:41: ISAKMP (0:3): processing NONCE payload. message ID = 0
23:43:41: ISAKMP (0:3): SKEYID state generated
23:43:41: ISAKMP (0:3): processing vendor id payload
23:43:41: ISAKMP (0:3): vendor ID seems Unity/DPD but bad major
23:43:41: ISAKMP (0:3): vendor ID is XAUTH
23:43:41: ISAKMP (0:3): SA is doing pre-shared key authentication
    using id type ID_IPV4_ADDR
23:43:41: ISAKMP (3): ID payload
    next-payload : 10
    type          : 1
    protocol      : 17
    port          : 500
    length        : 8

23:43:41: ISAKMP (3): Total payload length: 12
23:43:41: ISAKMP (0:3): sending packet to 10.64.10.28 (R) AG_INIT_EXCH
23:43:41: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_READY New State = IKE_R_AM2
23:43:42: ISAKMP (0:3): received packet from 10.64.10.28 (R) AG_INIT_EXCH
23:43:42: ISAKMP (0:3): processing HASH payload. message ID = 0
23:43:42: ISAKMP (0:3): SA has been authenticated with 10.64.10.28
23:43:42: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE
23:43:43: ISAKMP (0:3): received packet from 10.64.10.28 (R) QM_IDLE
23:43:43: ISAKMP (0:3): Need config/address
23:43:43: ISAKMP (0:3): Need config/address
23:43:43: ISAKMP: Sending private address: 10.1.2.2
23:43:43: ISAKMP (0:3): initiating peer config to 10.64.10.28.
    ID = -1082015193
23:43:43: ISAKMP (0:3): sending packet to 10.64.10.28 (R) CONF_ADDR
23:43:43: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_MODE_SET_SENT
23:43:43: ISAKMP (0:3): received packet from 10.64.10.28 (R) CONF_ADDR
23:43:43: ISAKMP (0:3): processing transaction payload from 10.64.10.28.
    message ID = -1082015193
23:43:43: ISAKMP: Config payload ACK
23:43:43: ISAKMP (0:3): peer accepted the address!
23:43:43: ISAKMP (0:3): deleting node -1082015193 error FALSE
    reason "done with transaction"
23:43:43: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK
Old State = IKE_CONFIG_MODE_SET_SENT New State = IKE_P1_COMPLETE
23:43:43: ISAKMP (0:3): Delaying response to QM request.
23:43:43: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
23:43:44: ISAKMP (0:3): received packet from 10.64.10.28 (R) QM_IDLE
23:43:44: ISAKMP (0:3): processing HASH payload. message ID = -920829332
23:43:44: ISAKMP (0:3): processing SA payload. message ID = -920829332
23:43:44: ISAKMP (0:3): Checking IPsec proposal 1
23:43:44: ISAKMP: transform 1, ESP_DES
23:43:44: ISAKMP: attributes in transform:
23:43:44: ISAKMP: authenticator is HMAC-MD5
23:43:44: ISAKMP: encaps is 1
    !--- Proposed Phase 2 transform set !--- matched configured IPsec transform set. 23:43:44:
ISAKMP (0:3): atts are acceptable.
23:43:44: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 10.64.10.46, remote= 10.64.10.28,
local_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.1.2.2/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysizes= 0, flags= 0x4
23:43:44: ISAKMP (0:3): processing NONCE payload. message ID = -920829332
```



```

23:43:44: ISAKMP (0:3): processing ID payload. message ID = -920829332
23:43:44: ISAKMP (0:3): processing ID payload. message ID = -920829332
23:43:44: ISAKMP (0:3): asking for 1 spis from ipsec
23:43:44: ISAKMP (0:3): Node -920829332,
    Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
23:43:44: IPSEC(key_engine): got a queue event...
23:43:44: IPSEC(spi_response): getting spi 2940839732 for SA
from 10.64.10.46 to 10.64.10.28 for prot 3
23:43:44: ISAKMP: received ke message (2/1)
23:43:45: ISAKMP (0:3): sending packet to 10.64.10.28 (R) QM_IDLE
23:43:45: ISAKMP (0:3): Node -920829332,
    Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
23:43:45: ISAKMP (0:3): received packet from 10.64.10.28 (R) QM_IDLE
23:43:45: ISAKMP (0:3): Creating IPsec SAs
23:43:45: inbound SA from 10.64.10.28 to 10.64.10.46
    (proxy 10.1.2.2 to 192.168.10.0)
23:43:45: has spi 0xAF49A734 and conn_id 200 and flags 4
23:43:45: outbound SA from 10.64.10.46 to 10.64.10.28
    (proxy 192.168.10.0 to 10.1.2.2 )
23:43:45: has spi 1531785085 and conn_id 201 and flags C
23:43:45: ISAKMP (0:3): deleting node 1961959105 error FALSE
    reason "saved qm no longer needed"
23:43:45: ISAKMP (0:3): deleting node -920829332 error FALSE
    reason "quick mode done (await())"
23:43:45: ISAKMP (0:3): Node -920829332,
    Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
23:43:45: IPSEC(key_engine): got a queue event...
23:43:45: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.64.10.46, remote= 10.64.10.28,
local_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.1.2.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0xAF49A734(2940839732), conn_id= 200, keysize= 0, flags= 0x4
23:43:45: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.64.10.46, remote= 10.64.10.28,
local_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.1.2.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x5B4D2F7D(1531785085), conn_id= 201, keysize= 0, flags= 0xC
!--- IPsec SAs created. 23:43:45: IPSEC(create_sa): sa created, (sa) sa_dest= 10.64.10.46,
sa_prot= 50, sa_spi= 0xAF49A734(2940839732),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 200
23:43:45: IPSEC(create_sa): sa created, (sa) sa_dest= 10.64.10.28,
sa_prot= 50, sa_spi= 0x5B4D2F7D(1531785085),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 201
23:43:45: ISAKMP: received ke message (4/1)
23:43:45: ISAKMP: Locking CONFIG struct 0x8180BEF4
    for crypto_ikmp_config_handle_kei_mess, count 3
23:43:50: ISAKMP (0:2): purging node 618568216
23:43:50: ISAKMP (0:2): purging node -497663485
23:44:00: ISAKMP (0:2): purging SA., sa=816B5724, delme=816B5724
23:44:00: ISAKMP: Unlocking CONFIG struct 0x8180BEF4 on
    return of attributes, count 2

```

[Дополнительные сведения](#)

- [Страница поддержки RADIUS](#)

- [Страница поддержки Cisco Secure ACS для Windows](#)
- [Страница поддержки Cisco Secure ACS для UNIX](#)
- [Страница поддержки IPSec](#)
- [Запросы комментариев \(RFC\)](#)
- [Техническая поддержка - Cisco Systems](#)