Содержание

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 versionCisco Internetwork Operating System SoftwareIOS (tm) C2600 Software (C2600-
JK9O3S-M), Version 12.2(8)T,   RELEASE SOFTWARE (fc2)TAC Support:
http://www.cisco.com/tacCopyright (c) 1986-2002 by cisco Systems, Inc.Compiled Thu 14-Feb-02
16:50 by ccaiImage text-base: 0x80008070, data-base: 0x81816184ROM: System Bootstrap, Version
11.3(2)XA4, RELEASE SOFTWARE (fc1)vpn2611 uptime is 1 hour, 15 minutesSystem returned to ROM by
reloadSystem 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 49Bridging 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

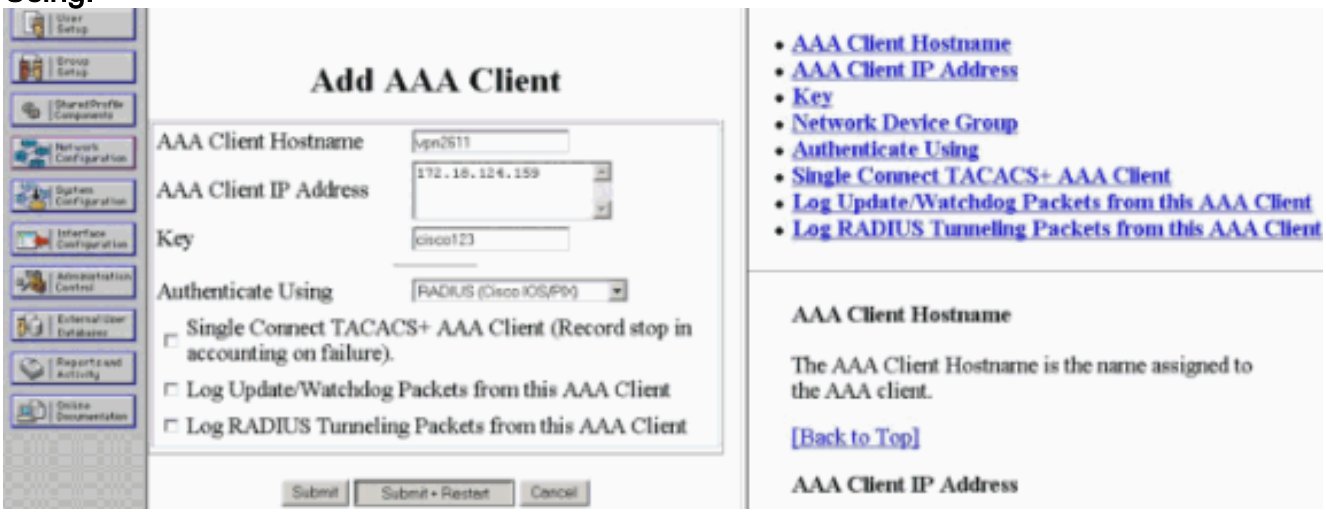
```
vpn2611#show runBuilding configuration...Current
configuration : 1884 bytes!version 12.2service
timestamps debug uptimeservice timestamps log uptimeno
service password-encryption!hostname vpn2611!!--- Enable
AAA for user authentication and group authorization.aaa
new-model!!--- In order to enable 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 logip audit po max-events 100!!--- Create an
Internet Security Association and !--- Key Management
Protocol (ISAKMP) policy for Phase 1 negotiations.crypto
isakmp policy 3encr 3desauthentication pre-sharegroup
2!!!--- Create the Phase 2 policy for actual data
encryption.crypto ipsec transform-set myset esp-3des
esp-sha-hmac!!--- Create a dynamic map and !--- apply
the transform set that was created.crypto dynamic-map
dynmap 10set transform-set myset!!--- Create the actual
crypto map, !--- and apply the AAA lists that were
created earlier.crypto map clientmap client
authentication list userauthencrypto map clientmap
isakmp authorization list groupauthorcrypto map
clientmap client configuration address respondcrypto map
clientmap 10 ipsec-isakmp dynamic dynmap!!fax interface-
type fax-mailmta receive maximum-recipients 0!!!!--
Apply the crypto map on the outside interface.interface
Ethernet0/0ip 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 10.16.20.200ip classlessip
route 0.0.0.0 0.0.0.0 10.1.1.2ip http serverip 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
cisco123radius-server retransmit 3call rsvp-sync!!mgcp
profile default!dial-peer cor custom!!!!!line con 0
exec-timeout 0 0line aux 0line vty 0 4!!endvpn2611#
```

Конфигурация сервера RADIUS

Настройте сервер RADIUS для клиентов AAA (маршрутизатор)

Выполните следующие действия:

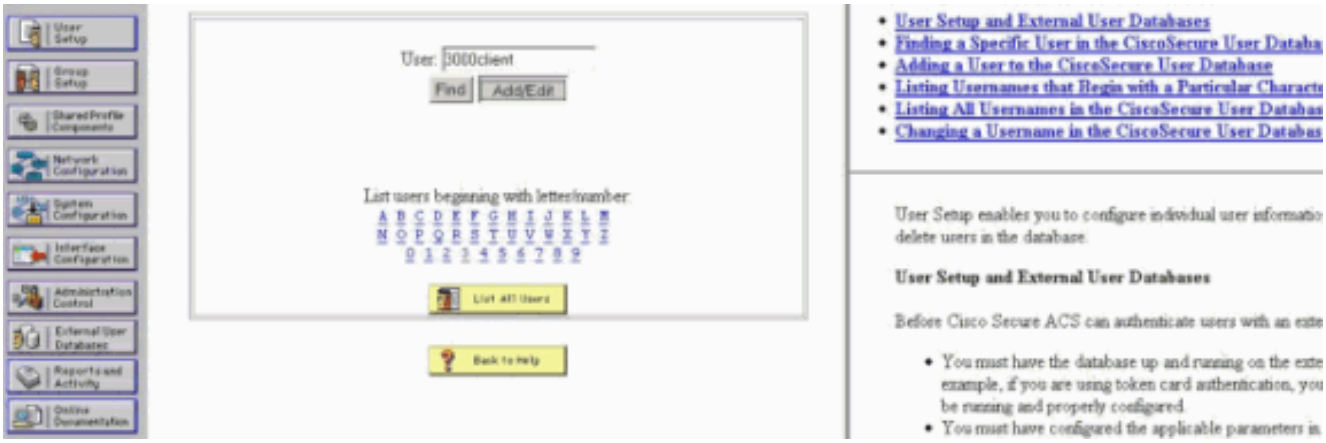
1. **Нажмите Add Запись** для добавления маршрутизатора к Базе данных сервера RADIUS.
2. **Установите IP-адрес маршрутизатора 172.18.124.159, а также общий секретный ключ "cisco123" и выберите RADIUS в раскрывающемся меню Authenticate Using.**



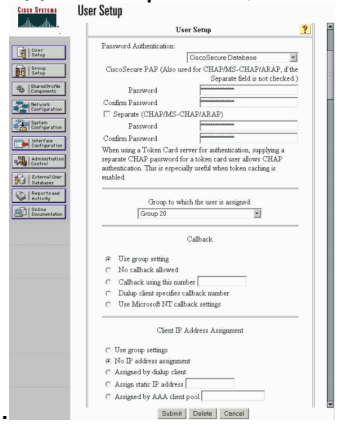
Настройте сервер RADIUS для групповой аутентификации и авторизации

Выполните следующие действия:

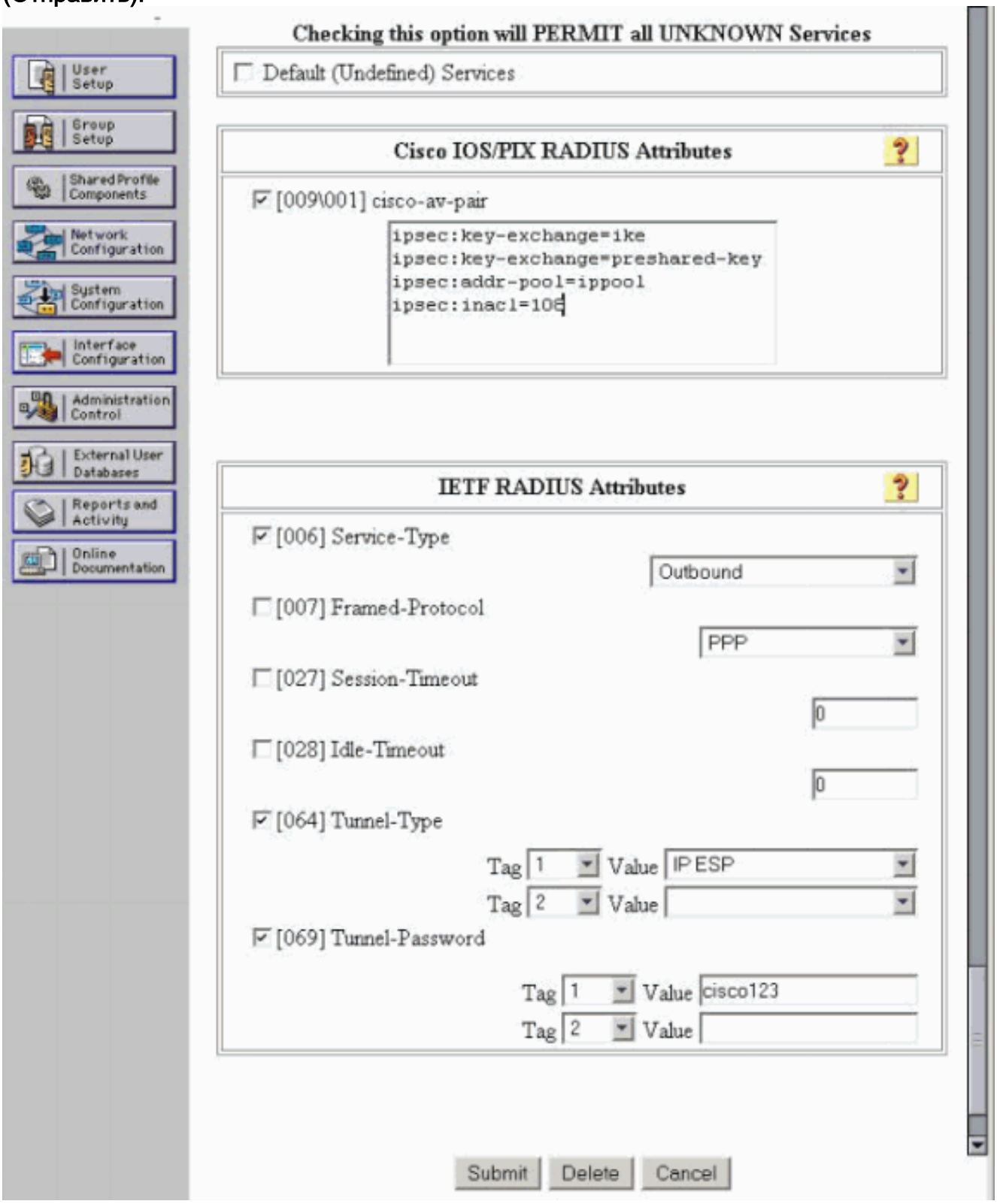
1. Нажмите **Add/Edit** для добавления Пользователя, названного **3000client** к серверу RADIUS.



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**.



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=ikeipsec:key-exchange=preshared-keyipsec:addr-pool=ippoolipsec:inacl=108 (нужно только в случае, если вы используете на маршрутизаторе разделенное тунеллирование)Также убедитель, что аттрибуты heseg IETF RADIUS Attributes включены (задействованы):Атрибут 6: Service-Type=OutboundАтрибут 64: Tunnel-Type=IP ESPАтрибут 69: Tunnel-Password=cisco123 (это - ваш пароль группы на Клиенте VPN),**По завершении нажмите кнопку Submit (Отправить).**



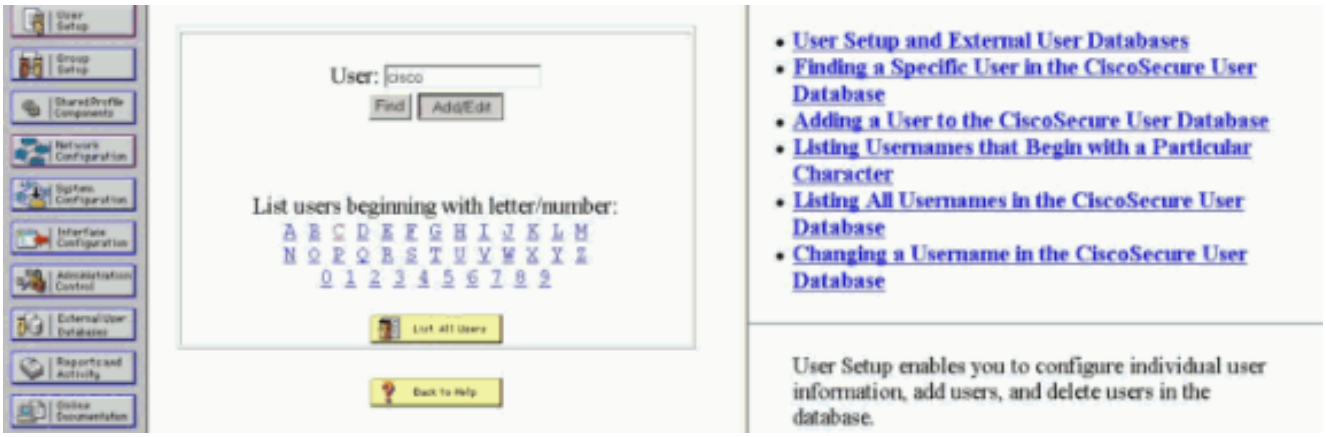
Под Определяемыми поставщиком Атрибутами можно также включить эти

необязательные атрибуты:ipsec:default-домен =ipsec:timeout =ipsec:idletime =ipsec:dns-серверы =ipsec:wins-серверы =

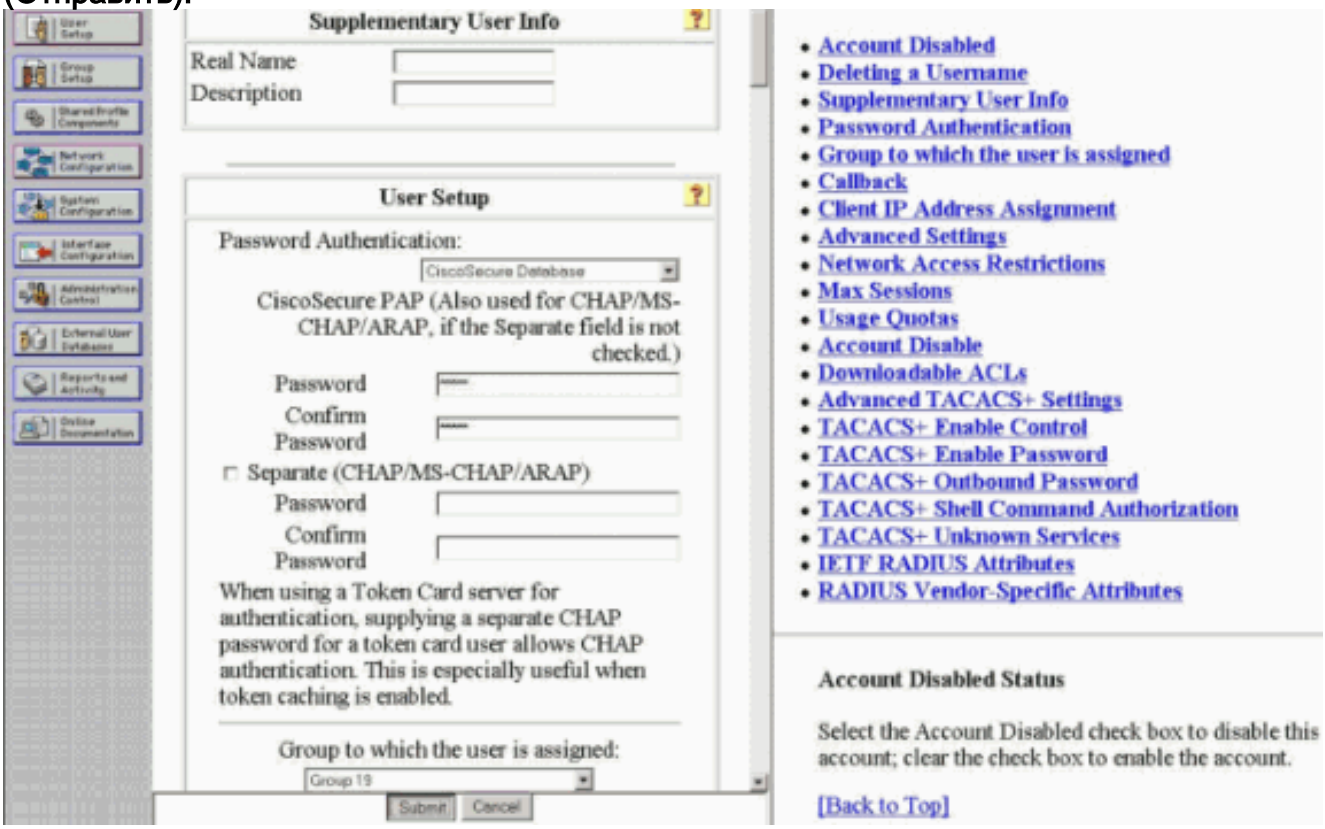
Настройка сервера RADIUS для аутентификации пользователей

Выполните следующие действия:

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



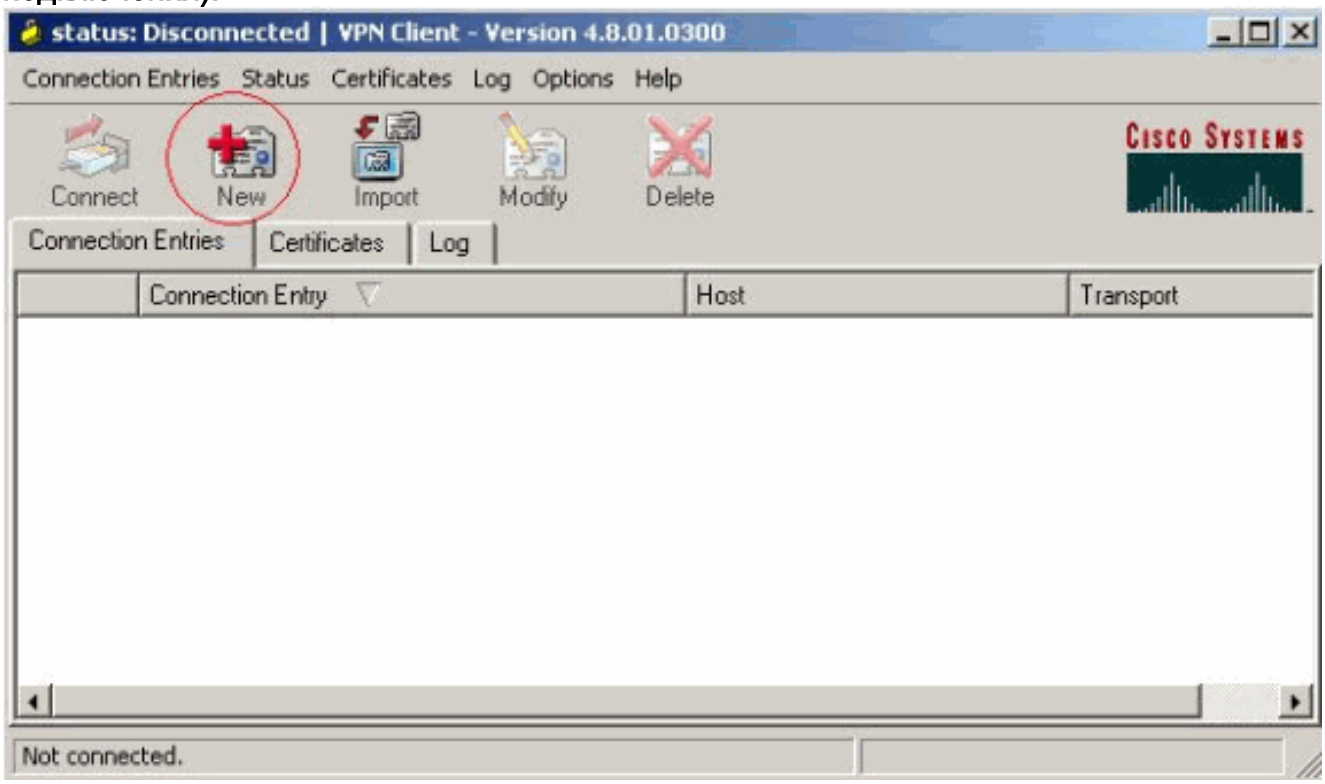
2. **В следующем окне определите пароль для пользователя cisco.** Пароль является также **Cisco**.Учетную запись пользователя можно включить в группу. **По завершении нажмите кнопку Submit**
(Отправить).



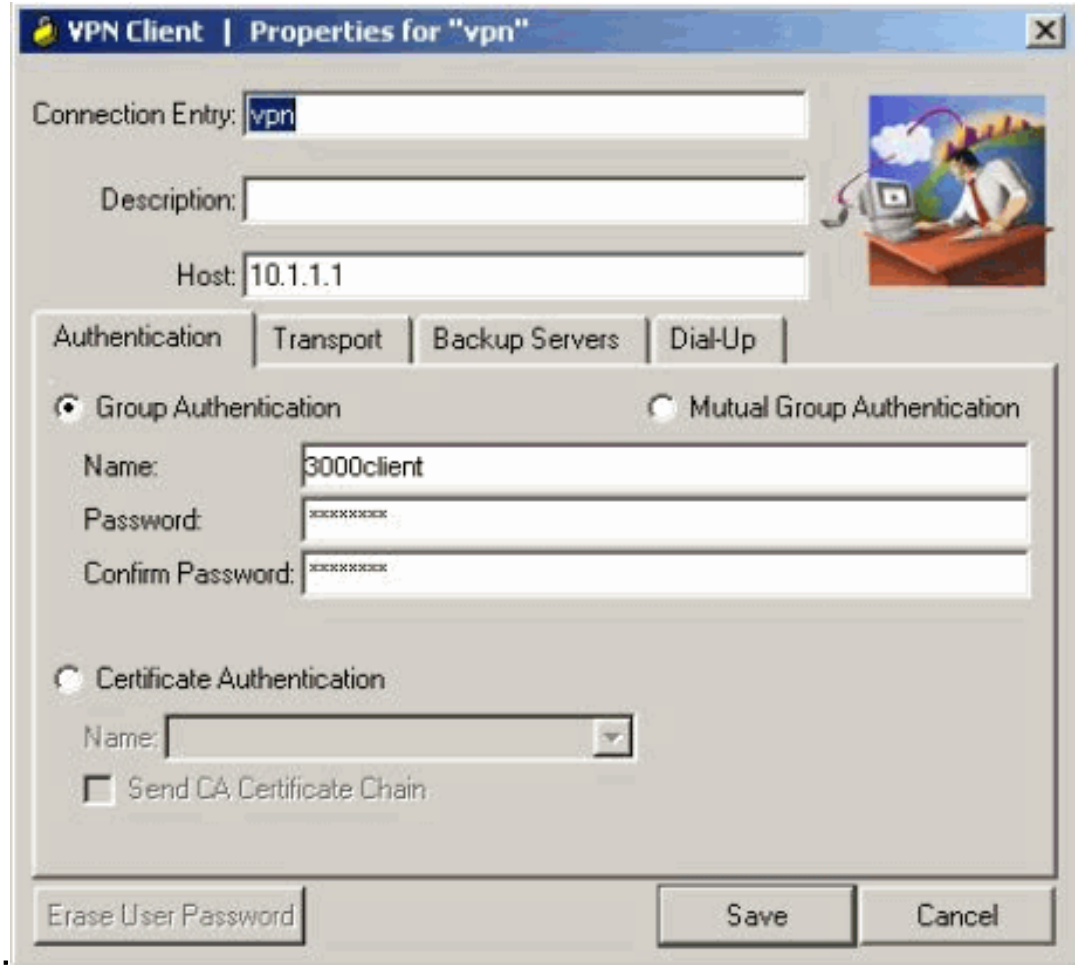
Настройка VPN Client 4.8

Чтобы настроить VPN Client 4.8, выполните следующие действия:

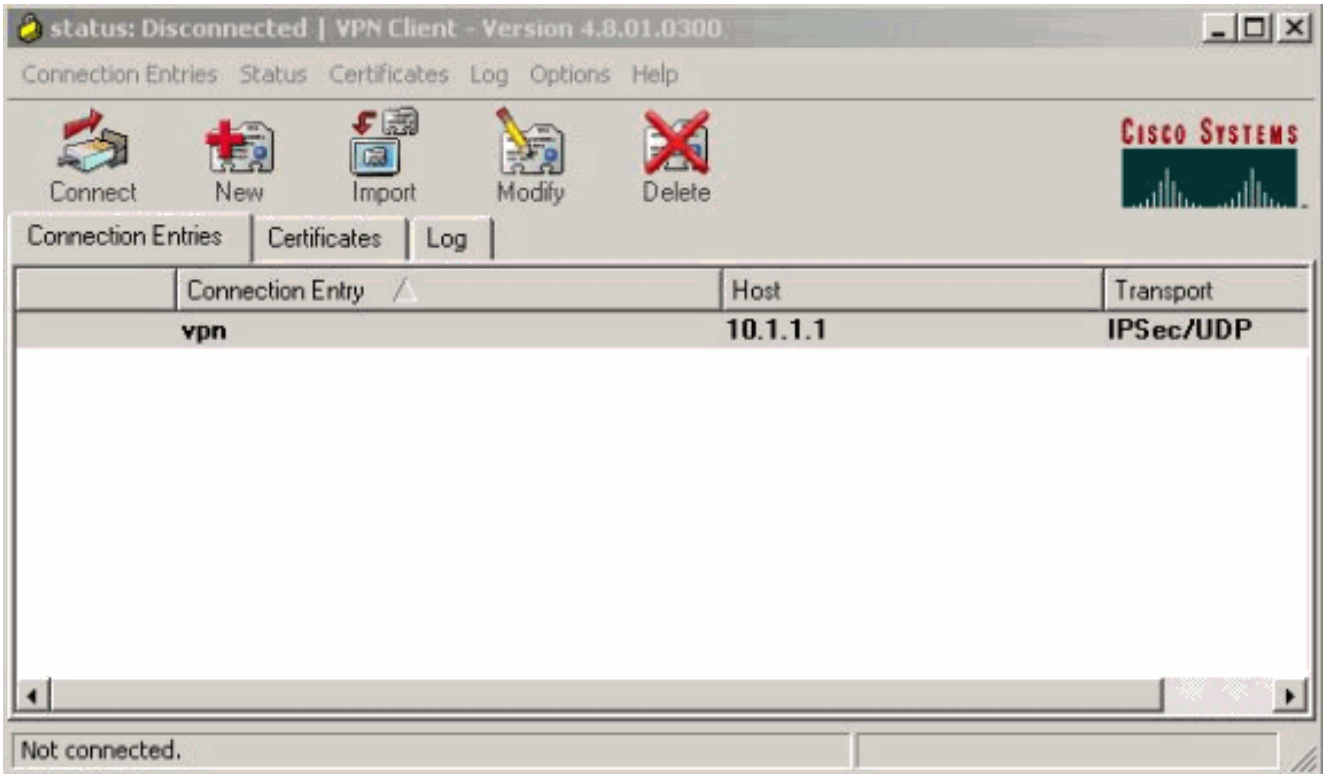
1. Выберите Пуск > Программы > Cisco Systems VPN Client > VPN Client.
2. Нажмите кнопку New (Создать), чтобы открыть окно Create New VPN Connection Entry (Создание записи нового VPN-подключения).



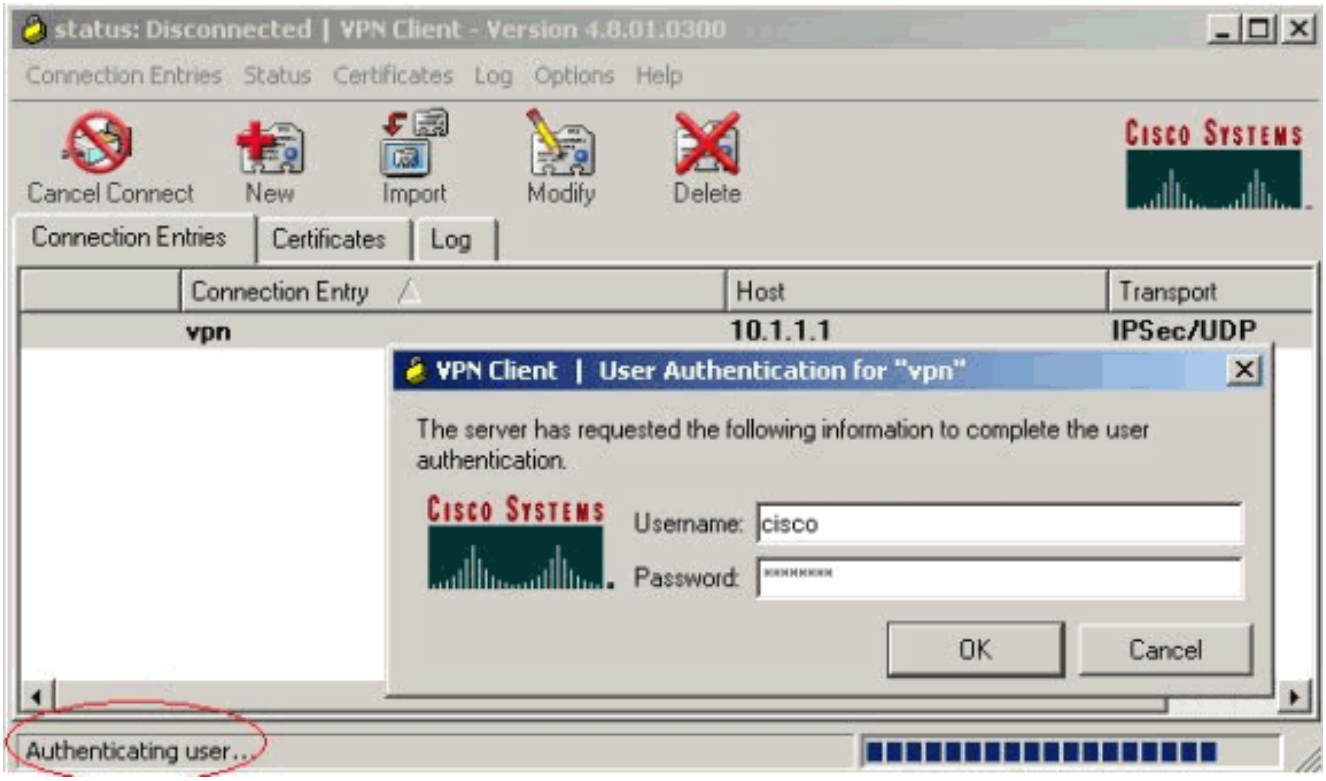
3. Введите имя записи и описание подключения. Введите внешний IP-адрес маршрутизатора в поле Host (Хост). Затем введите имя группы VPN и нажмите кнопку Save (Сохранить).



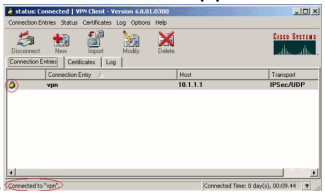
4. Щелкните по соединению, вы хотите использовать и нажать **Connect** от главного окна VPN
   Client.



5. **При появлении соответствующего запроса введите имя пользователя и пароль для аутентификации Xauth и нажмите OK 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 sadst             src             state          conn-id
slot10.1.1.1  10.0.0.1   QM_IDLE              3       0vpn2611#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        02000 Ethernet0/0
10.1.1.1  set    HMAC_SHA+3DES_56_C        0        52001 Ethernet0/0     10.1.1.1  set
HMAC_SHA+3DES_56_C        5        02002 Ethernet0/0     10.1.1.1  set    HMAC_SHA+3DES_56_C
0        62003 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: Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

- 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 debugGeneral OS:AAA Authorization debugging is onRadius protocol debugging is onRadius packet protocol debugging is onCryptographic Subsystem:Crypto ISAKMP debugging is onCrypto IPSEC debugging is onvpn2611#1w0d: ISAKMP (0:0): received packet from 10.0.0.1 (N) NEW SA1w0d: ISAKMP: local port 500, remote port 5001w0d: ISAKMP (0:2): (Re)Setting client xauth list userauthen and state1w0d: ISAKMP: Locking CONFIG struct 0x830BF118 from crypto_ikmp_config_initialize_sa, count 21w0d: ISAKMP (0:2): processing SA payload. message ID = 01w0d: ISAKMP (0:2): processing ID payload. message ID = 01w0d: ISAKMP (0:2): processing vendor id payload1w0d: ISAKMP (0:2): vendor ID seems Unity/DPD but bad major1w0d: ISAKMP (0:2): vendor ID is XAUTH1w0d: ISAKMP (0:2): processing vendor id payload1w0d: ISAKMP (0:2): vendor ID is DPD1w0d: ISAKMP (0:2): processing vendor id payload1w0d: ISAKMP (0:2): vendor ID is Unity1w0d: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 3 policy1w0d: ISAKMP: encryption 3DES-CBC1w0d: ISAKMP: hash SHA1w0d: ISAKMP: default group 21w0d: ISAKMP: auth XAUTHInitPreShared1w0d: ISAKMP: life type in seconds1w0d: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: ISAKMP (0:2): atts are acceptable. Next payload is 31w0d: ISAKMP (0:2): processing KE payload. message ID = 01w0d: ISAKMP (0:2): processing NONCE payload. message ID = 01w0d: ISAKMP (0:2): processing vendor id payload1w0d: ISAKMP (0:2): processing vendor id payload1w0d: ISAKMP (0:2): processing vendor id payload1w0d: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-11w0d: 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_EXCHOld 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=NET1w0d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(66832552) user='3000client'1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): send AV service=ike1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): send AV protocol=ipsec1w0d: 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 data1w0d: RADIUS: ustruct sharecount=31w0d: Radius: radius_port_info() success=0 radius_nas_port=11w0d: RADIUS: Send to ISAKMP-ID-AUTH id 60 172.18.124.96:1645, Access-Request, len 831w0d: RADIUS: authenticator AF EC D3 AD D6 39 4F 7D - A0 5E FC 64 F5 DE A7 3B1w0d: 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 1761w0d: RADIUS: authenticator 52 BA 0A 38 AC C2 2B 6F - A0 77 64 93 D6 19 78 CF1w0d: 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 831986481w0d: 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
```

091w0d: RADIUS: TAS(1) created and enqueued.1w0d: RADIUS: Tunnel-Password decrypted, [01] cisco1231w0d: RADIUS: TAS(1) takes precedence over tagged attributes, tunnel_type=esp1w0d: RADIUS: free TAS(1)1w0d: AAA/AUTHOR (66832552): Post authorization status = PASS_REPL1w0d: ISAKMP: got callback 1AAA/AUTHOR/IKE: Processing AV key-exchange=ikeAAA/AUTHOR/IKE: Processing AV key-exchange=preshared-keyAAA/AUTHOR/IKE: Processing AV addr-pool=ippoolAAA/AUTHOR/IKE: Processing AV inacl=108AAA/AUTHOR/IKE: Processing AV tunnel-type*espAAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123AAA/AUTHOR/IKE: Processing AV tunnel-tag*11w0d: ISAKMP (0:2): SKEYID state generated1w0d: ISAKMP (0:2): SA is doing pre-shared key authentication plux XAUTH using id type ID_IPV4_ADDR1w0d: ISAKMP (2): ID payloadnext-payload : 10type : 1protocol : 17port : 500length : 81w0d: ISAKMP (2): Total payload length: 121w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) AG_INIT_EXCH1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLYOld 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=01w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) AG_INIT_EXCH1w0d: ISAKMP (0:2): processing HASH payload. message ID = 01w0d: ISAKMP (0:2): processing NOTIFY INITIAL_CONTACT protocol 1spi 0, message ID = 0, sa = 831938B01w0d: ISAKMP (0:2): Process initial contact, bring down existing phase 1 and 2 SA's1w0d: ISAKMP (0:2): returning IP addr to the address pool: 10.16.20.11w0d: ISAKMP (0:2): returning address 10.16.20.1 to pool1w0d: ISAKMP (0:2): peer does not do paranoid keepalives.1w0d: ISAKMP (0:2): SA has been authenticated with 10.0.0.11w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM_IDLE 1w0d: ISAKMP (0:2): purging node -13775376281w0d: ISAKMP: Sending phase 1 responder lifetime 864001w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCHOld 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 ISAKMP1w0d: IPSEC(key_engine_delete_sas): delete all SAs shared with 10.0.0.1 1w0d: ISAKMP (0:2): Need XAUTH1w0d: AAA: parse name=ISAKMP idb type=-1 tty=-11w0d: AAA/MEMORY: create_user (0x830CAF28) user='NULL' ruser='NULL' ds0=0 port='ISAKMP' rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN priv=0 initial_task_id='0'1w0d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETEOld State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT 1w0d: ISAKMP: got callback 11w0d: ISAKMP/xauth: request attribute XAUTH_TYPE_V21w0d: ISAKMP/xauth: request attribute XAUTH_MESSAGE_V21w0d: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V21w0d: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V21w0d: ISAKMP (0:2): initiating peer config to 10.0.0.1. ID = -10218891931w0d: 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_LOGINOld State = IKE_XAUTH_AAA_START_LOGIN_AWAIT New State = IKE_XAUTH_REQ_SENT 1w0d: ISAKMP (0:1): purging node 8322385981w0d: ISAKMP (0:1): purging node 19132254911w0d: 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 = -10218891931w0d: ISAKMP: Config payload REPLY1w0d: ISAKMP/xauth: reply attribute XAUTH_TYPE_V2 unexpected1w0d: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V21w0d: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V21w0d: 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_REPLYOld State = IKE_XAUTH_REQ_SENT New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT 1w0d: RADIUS: ustruct sharecount=21w0d: 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 C01w0d: 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 6E1w0d: RADIUS: Framed-IP-Address [8] 6 255.255.255.255 1w0d: RADIUS: saved authorization data for user 830CAF28 at 830F89F81w0d: ISAKMP: got callback 11w0d: ISAKMP (0:2): initiating peer config to 10.0.0.1. ID = -5471893281w0d: 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_LOGINOld 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=01w0d: 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 = -5471893281w0d: ISAKMP: Config payload ACK1w0d: ISAKMP (0:2): XAUTH ACK Processed1w0d: ISAKMP (0:2): deleting node -547189328 error FALSE reason "done with transaction"1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACKOld State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE 1w0d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETEOld 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 = -19111892011w0d: ISAKMP: Config payload REQUEST1w0d: ISAKMP (0:2): checking request:1w0d: ISAKMP: IP4_ADDRESS1w0d: ISAKMP: IP4_NETMASK1w0d: ISAKMP: IP4_DNS1w0d: ISAKMP: IP4_NBNS1w0d: ISAKMP:

ADDRESS_EXPIRY1w0d: ISAKMP: APPLICATION_VERSION1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x70001w0d: ISAKMP: UNKNOWN Unknown Attr: 0x70011w0d: ISAKMP: DEFAULT_DOMAIN1w0d: ISAKMP: SPLIT_INCLUDE1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x70071w0d: ISAKMP: UNKNOWN Unknown Attr: 0x70081w0d: ISAKMP: UNKNOWN Unknown Attr: 0x70051w0d: AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-11w0d: 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_REQUESTOld 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=NET1w0d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(3098118746) user='3000client'1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): send AV service=ike1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): send AV protocol=ipsec1w0d: 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 data1w0d: RADIUS: ustruct sharecount=31w0d: Radius: radius_port_info() success=0 radius_nas_port=11w0d: RADIUS: Send to ISAKMP-GROUP-AUTH id 62 172.18.124.96:1645, Access-Request, len 831w0d: RADIUS: authenticator 32 C5 32 FF AB B7 E4 68 - 9A 68 5A DE D5 56 0C BE1w0d: 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 1761w0d: RADIUS: authenticator DF FA FE 21 07 92 4F 10 - 75 5E D6 96 66 70 19 271w0d: 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 83143E641w0d: 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 091w0d: RADIUS: TAS(1) created and enqueued.1w0d: RADIUS: Tunnel-Password decrypted, [01] cisco1231w0d: RADIUS: TAS(1) takes precedence over tagged attributes, tunnel_type=esp1w0d: RADIUS: free TAS(1)1w0d: AAA/AUTHOR (3098118746): Post authorization status = PASS_REPL1w0d: ISAKMP: got callback 1AAA/AUTHOR/IKE: Processing AV key-exchange=ikeAAA/AUTHOR/IKE: Processing AV key-exchange=preshared-keyAAA/AUTHOR/IKE: Processing AV addr-pool=ippoolAAA/AUTHOR/IKE: Processing AV inacl=108AAA/AUTHOR/IKE: Processing AV tunnel-type*espAAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123AAA/AUTHOR/IKE: Processing AV tunnel-tag*11w0d: ISAKMP (0:2): attributes sent in message:1w0d: Address: 0.2.0.01w0d: ISAKMP (0:2): allocating address 10.16.20.21w0d: ISAKMP: Sending private address: 10.16.20.21w0d: ISAKMP: Unknown Attr: IP4_NETMASK (0x2)1w0d: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 863951w0d: 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/tacCopyright (c) 1986-2002 by cisco Systems, Inc.Compiled Thu 14-Feb-02 16:50 by ccai1w0d: 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 01w0d: 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 = -19111892011w0d: 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_ATTROld 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=01w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE 1w0d: ISAKMP (0:2): processing HASH payload. message ID = 1325572811w0d: ISAKMP (0:2): processing SA payload. message ID = 1325572811w0d: ISAKMP (0:2): Checking IPSec proposal 11w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-MD51w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 01w0d: ISAKMP (0:2): skipping next ANDed proposal (1)1w0d: ISAKMP (0:2): Checking IPSec proposal 21w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-SHA1w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: ISAKMP (0:2): atts are acceptable.1w0d: ISAKMP (0:2): Checking IPSec proposal 21w0d: ISAKMP (0:2): transform 1, IPPCP LZS1w0d: ISAKMP: attributes in transform:1w0d:

ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: IPSEC(validate_proposal): transform proposal (prot 4, trans 3, hmac_alg 0) not supported1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 01w0d: ISAKMP (0:2): Checking IPSec proposal 31w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-MD51w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 01w0d: ISAKMP (0:2): Checking IPSec proposal 41w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-SHA1w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: 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= 0x41w0d: ISAKMP (0:2): processing NONCE payload. message ID = 1325572811w0d: ISAKMP (0:2): processing ID payload. message ID = 1325572811w0d: ISAKMP (0:2): processing ID payload. message ID = 1325572811w0d: ISAKMP (0:2): asking for 1 spis from ipsec1w0d: ISAKMP (0:2): Node 132557281, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCHOld 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 31w0d: 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_MESG_FROM_IPSEC, IKE_SPI_REPLYOld 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 SAs1w0d: 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 41w0d: lifetime of 2147483 seconds1w0d: 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 C1w0d: 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_MESG_FROM_PEER, IKE_QM_EXCHOld 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= 0x41w0d: 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= 0xC1w0d: 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= 20001w0d: 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= 20011w0d: ISAKMP: received ke message (4/1)1w0d: ISAKMP: Locking CONFIG struct 0x830BF118 for crypto_ikmp_config_handle_kei_mess, count 31w0d: ISAKMP (0:1): purging SA., sa=83196748, delme=831967481w0d: ISAKMP: Unlocking CONFIG struct 0x830BF118 on return of attributes, count 21w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE 1w0d: ISAKMP (0:2): processing HASH payload. message ID = -12733329081w0d: ISAKMP (0:2): processing SA payload. message ID = -12733329081w0d: ISAKMP (0:2): Checking IPSec proposal 11w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-MD51w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 01w0d: ISAKMP (0:2): skipping next ANDed proposal (1)1w0d: ISAKMP (0:2): Checking IPSec proposal 21w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-SHA1w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: ISAKMP (0:2): atts are acceptable.1w0d: ISAKMP (0:2): Checking IPSec proposal 21w0d: ISAKMP (0:2): transform 1, IPPCP LZS1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: IPSEC(validate_proposal): transform proposal (prot 4, trans 3, hmac_alg 0) not supported1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 01w0d: ISAKMP (0:2): Checking IPSec proposal 31w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-MD51w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 01w0d: ISAKMP (0:2): Checking IPSec proposal

41w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-SHA1w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: 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= 0x41w0d: ISAKMP (0:2): processing NONCE payload. message ID = -12733329081w0d: ISAKMP (0:2): processing ID payload. message ID = -12733329081w0d: ISAKMP (0:2): processing ID payload. message ID = -12733329081w0d: ISAKMP (0:2): asking for 1 spis from ipsec1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCHOld 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 10.0.0.1vpn2611#vpn2611#2 for prot 31w0d: 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_MESG_FROM_IPSEC, IKE_SPI_REPLYOld 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 SAs1w0d: 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 41w0d: lifetime of 2147483 seconds1w0d: 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 C1w0d: lifetime of 2147483 seconds**1w0d: ISAKMP (0:2): deleting node -1273332908 errovpn2611#un ar FALSE reason "quick mode done (await()"1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCHOld 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= 0x41w0d: 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-shllAll possible debugging has been turned offvpn2611#a-hmac , lifedur= 2147483s and 0kb, spi= 0x42FC1D6A(1123818858), conn_id= 2003, keysize= 0, flags= 0xC1w0d: 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= 20021w0d: 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 onRadius protocol debugging is onRadius packet protocol debugging is onCryptographic Subsystem:Crypto ISAKMP debugging is onCrypto 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 5001w0d: ISAKMP (0:2): (Re)Setting client xauth list userauthen and state1w0d: ISAKMP: Locking CONFIG struct 0x830BF118 from crypto_ikmp_config_initialize_sa, count 21w0d: ISAKMP (0:2): processing SA payload. message ID = 01w0d: ISAKMP (0:2): processing ID payload. message ID = 01w0d: ISAKMP (0:2): processing vendor id payload1w0d: ISAKMP (0:2): vendor ID seems Unity/DPD but bad major1w0d: ISAKMP (0:2): vendor ID is XAUTH1w0d: ISAKMP (0:2): processing vendor id payload1w0d: ISAKMP (0:2): vendor ID is DPD1w0d: ISAKMP (0:2): processing vendor id payload1w0d: ISAKMP (0:2): vendor ID is Unity1w0d: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 3 policy1w0d: ISAKMP: encryption 3DES-CBC1w0d: ISAKMP: hash SHA1w0d: ISAKMP: default group 21w0d: ISAKMP: auth XAUTHInitPreShared1w0d: ISAKMP: life type in seconds1w0d: 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 = 01w0d: ISAKMP (0:2): processing NONCE payload. message ID = 01w0d: ISAKMP (0:2): processing vendor id payload1w0d: ISAKMP (0:2): processing vendor id payload1w0d: ISAKMP (0:2): processing vendor id payload1w0d: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-11w0d: 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_EXCHOld 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=NET1w0d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(66832552) user='3000client'1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): send AV service=ike1w0d: 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 data1w0d: RADIUS: ustruct sharecount=31w0d: 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 3B1w0d: 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 CF1w0d: 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 831986481w0d: **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 091w0d: RADIUS: TAS(1) created and enqueued.1w0d: RADIUS: Tunnel-Password decrypted, [01] cisco123**1w0d: RADIUS: TAS(1) takes precedence over tagged attributes, tunnel_type=esp1w0d: RADIUS: free TAS(1)1w0d: AAA/AUTHOR (66832552): Post authorization status = PASS_REPL1w0d: ISAKMP: got callback 1AAA/AUTHOR/IKE: Processing AV key-exchange=ikeAAA/AUTHOR/IKE: Processing AV key-exchange=preshared-keyAAA/AUTHOR/IKE: Processing AV addr-pool=ippoolAAA/AUTHOR/IKE: Processing AV inacl=108AAA/AUTHOR/IKE: Processing AV tunnel-type*espAAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123AAA/AUTHOR/IKE: Processing AV tunnel-tag*11w0d: ISAKMP (0:2): SKEYID state generated1w0d: ISAKMP (0:2): SA is doing pre-shared key authentication plux XAUTH using id type ID_IPV4_ADDR1w0d: ISAKMP (2): ID payloadnext-payload : 10type : 1protocol : 17port : 500length : 81w0d: ISAKMP (2): Total payload length: 121w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) AG_INIT_EXCH1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLYOld 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=01w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) AG_INIT_EXCH1w0d: ISAKMP (0:2): processing HASH payload. message ID = 01w0d: ISAKMP (0:2): processing NOTIFY INITIAL_CONTACT protocol 1spi 0, message ID = 0, sa = 831938B01w0d: ISAKMP (0:2): Process initial contact, bring down existing phase 1 and 2 SA's1w0d: ISAKMP (0:2): returning IP addr to the address pool: 10.16.20.11w0d: ISAKMP (0:2): returning address 10.16.20.1 to pool1w0d: ISAKMP (0:2): peer does not do paranoid keepalives.1w0d: ISAKMP (0:2): SA has been authenticated with 10.0.0.11w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM_IDLE 1w0d: ISAKMP (0:2): purging node -13775376281w0d: ISAKMP: Sending phase 1 responder lifetime 864001w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCHOld 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 ISAKMP1w0d: IPSEC(key_engine_delete_sas): delete all SAs shared with 10.0.0.1 1w0d: ISAKMP (0:2): Need XAUTH1w0d: AAA: parse name=ISAKMP idb type=-1 tty=-11w0d: AAA/MEMORY: create_user (0x830CAF28) user='NULL' ruser='NULL' ds0=0 port='ISAKMP' rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN priv=0 initial_task_id='0'1w0d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETEOld State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT 1w0d: ISAKMP: got callback 11w0d: ISAKMP/xauth: request attribute XAUTH_TYPE_V21w0d: ISAKMP/xauth: request attribute XAUTH_MESSAGE_V21w0d: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V21w0d: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V21w0d: ISAKMP (0:2): initiating peer config to 10.0.0.1. ID = -102188919311w0d: 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_LOGINOld State = IKE_XAUTH_AAA_START_LOGIN_AWAIT New State = IKE_XAUTH_REQ_SENT 1w0d: ISAKMP (0:1): purging node 8322385981w0d: ISAKMP (0:1): purging node 191322549111w0d: 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 = -102188919311w0d: ISAKMP: Config payload REPLY1w0d: ISAKMP/xauth: reply attribute XAUTH_TYPE_V2 unexpected1w0d: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V21w0d: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V21w0d: 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_REPLYOld State = IKE_XAUTH_REQ_SENT New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT 1w0d: RADIUS: ustruct sharecount=21w0d: 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 721w0d: RADIUS: authenticator 98 12 4F C0 DA B9 48 B8 - 58 00 BA 14 08 8E 87 C01w0d: 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 6E1w0d: RADIUS: Framed-IP-Address [8] 6 255.255.255.255 1w0d: RADIUS: saved authorization data for user 830CAF28 at 830F89F81w0d: ISAKMP: got callback 11w0d: ISAKMP (0:2): initiating peer config to 10.0.0.1. ID = -5471893281w0d: 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_LOGINOld 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=01w0d: 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 = -5471893281w0d: ISAKMP: Config payload ACK1w0d: ISAKMP (0:2): XAUTH ACK Processed1w0d: ISAKMP (0:2): deleting node -547189328 error FALSE reason "done with transaction"1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACKOld State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE 1w0d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETEOld 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 = -19111892011w0d: ISAKMP: Config payload REQUEST1w0d: ISAKMP (0:2): checking request:1w0d: ISAKMP: IP4_ADDRESS1w0d: ISAKMP: IP4_NETMASK1w0d: ISAKMP: IP4_DNS1w0d: ISAKMP: IP4_NBNS1w0d: ISAKMP: ADDRESS_EXPIRY1w0d: ISAKMP: APPLICATION_VERSION1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x70001w0d: ISAKMP: UNKNOWN Unknown Attr: 0x70011w0d: ISAKMP: DEFAULT_DOMAIN1w0d: ISAKMP: SPLIT_INCLUDE1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x70071w0d: ISAKMP: UNKNOWN Unknown Attr: 0x70081w0d: ISAKMP: UNKNOWN Unknown Attr: 0x70051w0d: AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-11w0d: 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_REQUESTOld 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=NET1w0d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(3098118746) user='3000client'1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): send AV service=ike1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): send AV protocol=ipsec1w0d: 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 data1w0d: RADIUS: ustruct sharecount=31w0d: Radius: radius_port_info() success=0 radius_nas_port=11w0d: RADIUS: Send to ISAKMP-GROUP-AUTH id 62 172.18.124.96:1645, Access-Request, len 831w0d: RADIUS: authenticator 32 C5 32 FF AB B7 E4 68 - 9A 68 5A DE D5 56 0C BE1w0d: 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 1761w0d: RADIUS: authenticator DF FA FE 21 07 92 4F 10 - 75 5E D6 96 66 70 19 271w0d: 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 83143E641w0d: 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 091w0d: RADIUS: TAS(1) created and enqueued.1w0d: RADIUS: Tunnel-Password decrypted, [01] cisco1231w0d: RADIUS: TAS(1) takes precedence over tagged attributes, tunnel_type=esp1w0d: RADIUS: free TAS(1)1w0d: AAA/AUTHOR (3098118746): Post authorization status = PASS_REPL1w0d: ISAKMP: got callback 1AAA/AUTHOR/IKE: Processing AV key-exchange=ikeAAA/AUTHOR/IKE: Processing AV key-exchange=preshared-keyAAA/AUTHOR/IKE: Processing AV addr-pool=ippoolAAA/AUTHOR/IKE: Processing AV inacl=108AAA/AUTHOR/IKE: Processing AV tunnel-type*espAAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123AAA/AUTHOR/IKE: Processing AV tunnel-tag*11w0d: ISAKMP (0:2): attributes sent in message:1w0d: Address: 0.2.0.01w0d: ISAKMP (0:2): allocating address 10.16.20.21w0d: ISAKMP: Sending private address: 10.16.20.21w0d: ISAKMP: Unknown Attr: IP4_NETMASK (0x2)1w0d: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 863951w0d: 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/tacCopyright (c) 1986-2002 by cisco Systems, Inc.Compiled Thu 14-Feb-02

16:50 by ccai1w0d: 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 01w0d: 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 = -19111892011w0d: 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_ATTROld 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=01w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE 1w0d: ISAKMP (0:2): processing HASH payload. message ID = 1325572811w0d: ISAKMP (0:2): processing SA payload. message ID = 1325572811w0d: ISAKMP (0:2): Checking IPSec proposal 11w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-MD51w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 01w0d: ISAKMP (0:2): skipping next ANDed proposal (1)1w0d: ISAKMP (0:2): Checking IPSec proposal 21w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-SHA1w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: ISAKMP (0:2): atts are acceptable.1w0d: ISAKMP (0:2): Checking IPSec proposal 21w0d: ISAKMP (0:2): transform 1, IPPCP LZS1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: IPSEC(validate_proposal): transform proposal (prot 4, trans 3, hmac_alg 0) not supported1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 01w0d: ISAKMP (0:2): Checking IPSec proposal 31w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-MD51w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 01w0d: ISAKMP (0:2): Checking IPSec proposal 41w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-SHA1w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: 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= 0x41w0d: ISAKMP (0:2): processing NONCE payload. message ID = 1325572811w0d: ISAKMP (0:2): processing ID payload. message ID = 1325572811w0d: ISAKMP (0:2): processing ID payload. message ID = 1325572811w0d: ISAKMP (0:2): asking for 1 spis from ipsec1w0d: ISAKMP (0:2): Node 132557281, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCHOld 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 31w0d: 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_MESG_FROM_IPSEC, IKE_SPI_REPLYOld 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 SAs1w0d: 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 41w0d: lifetime of 2147483 seconds1w0d: 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 C1w0d: 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_MESG_FROM_PEER, IKE_QM_EXCHOld 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= 0x41w0d: 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= 0xC1w0d: 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= 20001w0d: 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= 20011w0d: ISAKMP: received ke message (4/1)1w0d: ISAKMP: Locking CONFIG struct 0x830BF118 for crypto_ikmp_config_handle_kei_mess, count 31w0d: ISAKMP (0:1): purging SA., sa=83196748,

delme=831967481w0d: ISAKMP: Unlocking CONFIG struct 0x830BF118 on return of attributes, count 21w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE 1w0d: ISAKMP (0:2): processing HASH payload. message ID = -12733329081w0d: ISAKMP (0:2): processing SA payload. message ID = -12733329081w0d: ISAKMP (0:2): Checking IPSec proposal 11w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-MD51w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 01w0d: ISAKMP (0:2): skipping next ANDed proposal (1)1w0d: ISAKMP (0:2): Checking IPSec proposal 21w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-SHA1w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: ISAKMP (0:2): atts are acceptable.1w0d: ISAKMP (0:2): Checking IPSec proposal 21w0d: ISAKMP (0:2): transform 1, IPPCP LZS1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: IPSEC(validate_proposal): transform proposal (prot 4, trans 3, hmac_alg 0) not supported1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 01w0d: ISAKMP (0:2): Checking IPSec proposal 31w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-MD51w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 01w0d: ISAKMP (0:2): Checking IPSec proposal 41w0d: ISAKMP: transform 1, ESP_3DES1w0d: ISAKMP: attributes in transform:1w0d: ISAKMP: authenticator is HMAC-SHA1w0d: ISAKMP: encaps is 11w0d: ISAKMP: SA life type in seconds1w0d: 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= 0x41w0d: ISAKMP (0:2): processing NONCE payload. message ID = -12733329081w0d: ISAKMP (0:2): processing ID payload. message ID = -12733329081w0d: ISAKMP (0:2): processing ID payload. message ID = -12733329081w0d: ISAKMP (0:2): asking for 1 spis from ipsec1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCHOld 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 10.0.0.1vpn2611#vpn2611#2 for prot 31w0d: 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_MESG_FROM_IPSEC, IKE_SPI_REPLYOld 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 SAs1w0d: 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 41w0d: lifetime of 2147483 seconds1w0d: 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 C1w0d: lifetime of 2147483 seconds**1w0d: ISAKMP (0:2): deleting node -1273332908 errovpn2611#un ar FALSE reason "quick mode done (await()"1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCHOld 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= 0x41w0d: 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-shllAll possible debugging has been turned offvpn2611#a-hmac , lifedur= 2147483s and 0kb, spi= 0x42FC1D6A(1123818858), conn_id= 2003, keysize= 0, flags= 0xC1w0d: 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= 20021w0d: 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