

Настройка IPSec для связи между двумя маршрутизаторами и клиентом Cisco VPN Client 4.x

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Проверка](#)

[Виртуальная частная сеть Cisco 2611](#)

[Cisco VPN 3640](#)

[Проверьте порядковые номера криптокарты](#)

[Устранение неполадок](#)

[Команды для устранения неполадок](#)

[Дополнительные сведения](#)

Введение

В этом документе показано, как конфигурировать IPSec между двумя маршрутизаторами Cisco и клиентом Cisco VPN 4.x. Операционная система Cisco IOS® Release 12.2(8)T и более поздних версий поддерживает соединения с Cisco VPN Client версии 3.x и более поздних.

[Для получения дополнительных сведений о динамическом назначении IP-адреса оконечному сетевому устройству другим оконечным сетевым устройством L2L-туннеля см. документ под названием Настройка соединения по протоколу IPsec между одноранговыми узлами с динамической маршрутизацией LAN-to-LAN и клиентами 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 общим ключом **cisco123** для Клиентов VPN
- Аутентификация группы и пользователя выполняется локально на маршрутизаторе для клиентов VPN.
- Для туннеля между локальными сетями используется параметр **no-xauth** для команды **ISAKMP key**.

Используемые компоненты

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

- Маршрутизатор под управлением операционной системы Cisco IOS Release 12.2(8)T. **Примечание:** Этот документ был недавно протестирован с программным обеспечением Cisco IOS версии 12.3(1). В связи с этим никаких изменений вносить не требуется.
- Cisco VPN Client для Windows версии 4.x (любая программа VPN Client версии 3.x и выше).

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.

Ниже приведены результаты выполнения команды `show version` на маршрутизаторе.

```
vpn2611#show version Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-JK9O3S-M), Version 12.2(8)T, RELEASE SOFTWARE (fc2) TAC Support: http://www.cisco.com/tac Copyright (c) 1986-2002 by cisco Systems, Inc. Compiled Thu 14-Feb-02 16:50 by ccai Image text-base: 0x80008070, data-base: 0x81816184 ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1) vpn2611 uptime is 1 hour, 15 minutes System returned to ROM by reload System image file is "flash:c2600-jk9o3s-mz.122-8.T" cisco 2611 (MPC860) processor (revision 0x203) with 61440K/4096K bytes of memory. Processor board ID JAD04370EEG (2285146560) M860 processor: part number 0, mask 49 Bridging software. X.25 software, Version 3.0.0. SuperLAT software (copyright 1990 by Meridian Technology Corp). TN3270 Emulation software. 2 Ethernet/IEEE 802.3 interface(s) 1 Serial network interface(s) 32K bytes of non-volatile configuration memory. 16384K bytes of processor board System flash (Read/Write) Configuration register is 0x2102
```

Условные обозначения

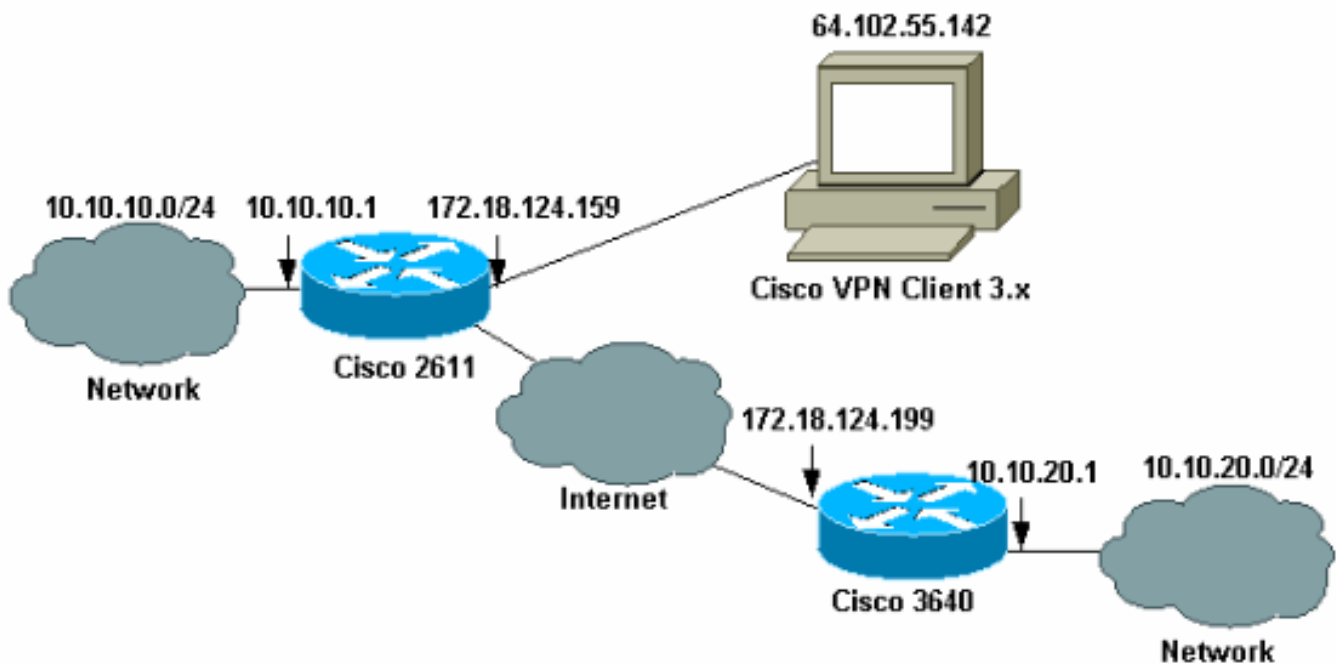
[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

Настройка

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

Схема сети

В настоящем документе используется следующая схема сети.



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

Конфигурации

Настройте маршрутизатор Cisco 2611

Маршрутизатор Cisco 2611

```
vpn2611#show run Building configuration... Current
configuration : 2265 bytes ! version 12.2 service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname vpn2611 ! !---
Enable AAA for user authentication !--- and group
authorization. aaa new-model ! ! !--- In order to enable
X-Auth for user authentication, !--- enable the aaa
authentication commands. aaa authentication login
userauthen local !--- In order to enable group
authorization, enable !--- the aaa authorization
commands. aaa authorization network groupauthor local
aaa session-id common ! !--- For local authentication of
the IPSec user, !--- create the user with a password.
username cisco password 0 cisco 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 for the VPN 3.x Clients. crypto isakmp
policy 3 encr 3des authentication pre-share group 2 ! !-
-- Create an ISAKMP policy for Phase 1 !--- negotiations
for the LAN-to-LAN tunnels. crypto isakmp policy 10 hash
md5 authentication pre-share !--- Specify the PreShared
key for the LAN-to-LAN tunnel. !--- Make sure that you
use the !--- no-xauth parameter with your ISAKMP key.
crypto isakmp key cisco123 address 172.18.124.199 no-
xauth ! !--- Create a group that is used to !--- specify
the WINS, DNS servers' address !--- to the client, along
with the pre-shared !--- key for authentication. crypto
```

```

isakmp client configuration group 3000client key
cisco123 dns 10.10.10.10 wins 10.10.10.20 domain
cisco.com pool ippool ! ! !--- Create the Phase 2 Policy
for actual data encryption. crypto ipsec transform-set
myset esp-3des esp-md5-hmac ! !--- Create a dynamic map
and apply !--- the transform set that was created
earlier. crypto dynamic-map dynmap 10 set transform-set
myset ! ! !--- Create the actual crypto map, and !---
apply the AAA lists that were created !--- earlier. Also
create a new instance for your !--- LAN-to-LAN tunnel.
Specify the peer IP address, !--- transform set, and an
Access Control List (ACL) for this !--- instance. crypto
map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor crypto map clientmap client configuration
address respond crypto map clientmap 1 ipsec-isakmp set
peer 172.18.124.199 set transform-set myset match
address 100 crypto map clientmap 10 ipsec-isakmp dynamic
dynmap ! ! fax interface-type fax-mail mta receive
maximum-recipients 0 ! ! !--- Apply the crypto map on
the outside interface. interface Ethernet0/0 ip address
172.18.124.159 255.255.255.0 half-duplex crypto map
clientmap ! interface Serial0/0 no ip address shutdown !
interface Ethernet0/1 ip address 10.10.10.1
255.255.255.0 no keepalive half-duplex ! ! !--- Create a
pool of addresses to be !--- assigned to the VPN
Clients. ip local pool ippool 14.1.1.100 14.1.1.200 ip
classless ip route 0.0.0.0 0.0.0.0 172.18.124.1 ip http
server ip pim bidir-enable ! ! !--- Create an ACL for
the traffic !--- to be encrypted. In this example, !---
the traffic from 10.10.10.0/24 to 10.10.20.0/24 !--- is
encrypted. access-list 100 permit ip 10.10.10.0
0.0.0.255 10.10.20.0 0.0.0.255 ! ! snmp-server community
foobar RO call rsvp-sync ! ! mgcp profile default !
dial-peer cor custom ! ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 ! ! end

```

[Настройте 3640 маршрутизаторов](#)

Маршрутизатор Cisco 3640

```

vpn3640#show run Building configuration... Current
configuration : 1287 bytes ! ! Last configuration change
at 13:47:37 UTC Wed Mar 6 2002 ! version 12.2 service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname vpn3640 ! ! ip
subnet-zero ip cef ! !--- Create an ISAKMP policy for
Phase 1 !--- negotiations for the LAN-to-LAN tunnels.
crypto isakmp policy 10 hash md5 authentication pre-
share ! !--- Specify the PreShared key for the LAN-to-LAN
!--- tunnel. You do not have to add the !--- X-Auth
parameter, as this !--- router does not do Cisco Unity
Client IPsec !--- authentication. crypto isakmp key
cisco123 address 172.18.124.159 ! ! !--- Create the
Phase 2 Policy for actual data encryption. crypto ipsec
transform-set myset esp-3des esp-md5-hmac ! !--- Create
the actual crypto map. Specify !--- the peer IP address,
transform !--- set, and an ACL for this instance. crypto
map mymap 10 ipsec-isakmp set peer 172.18.124.159 set
transform-set myset match address 100 ! call RSVP-sync !
! ! !--- Apply the crypto map on the outside interface.
interface Ethernet0/0 ip address 172.18.124.199
255.255.255.0 half-duplex crypto map mymap ! interface

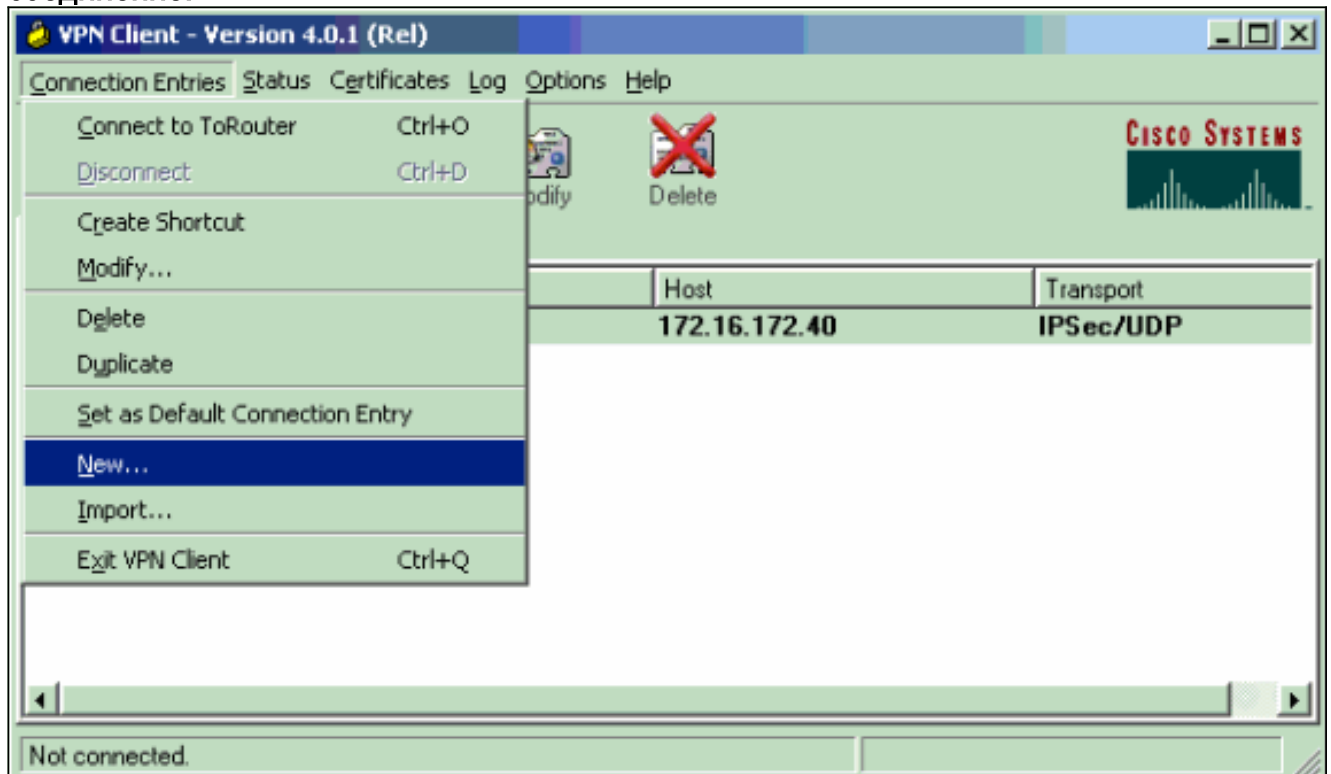
```

```
Ethernet0/1 ip address 10.10.20.1 255.255.255.0 half-  
duplex ! ip classless ip route 0.0.0.0 0.0.0.0  
172.18.124.1 ip http server ip pim bidir-enable ! !---  
Create an ACL for the traffic to !--- be encrypted. In  
this example, !--- the traffic from 10.10.20.0/24 to  
10.10.10.0/24 !--- is encrypted. access-list 100 permit  
ip 10.10.20.0 0.0.0.255 10.10.10.0 0.0.0.255 snmp-server  
community foobar RO ! dial-peer cor custom ! ! line con  
0 exec-timeout 0 0 line aux 0 line vty 0 4 login ! end
```

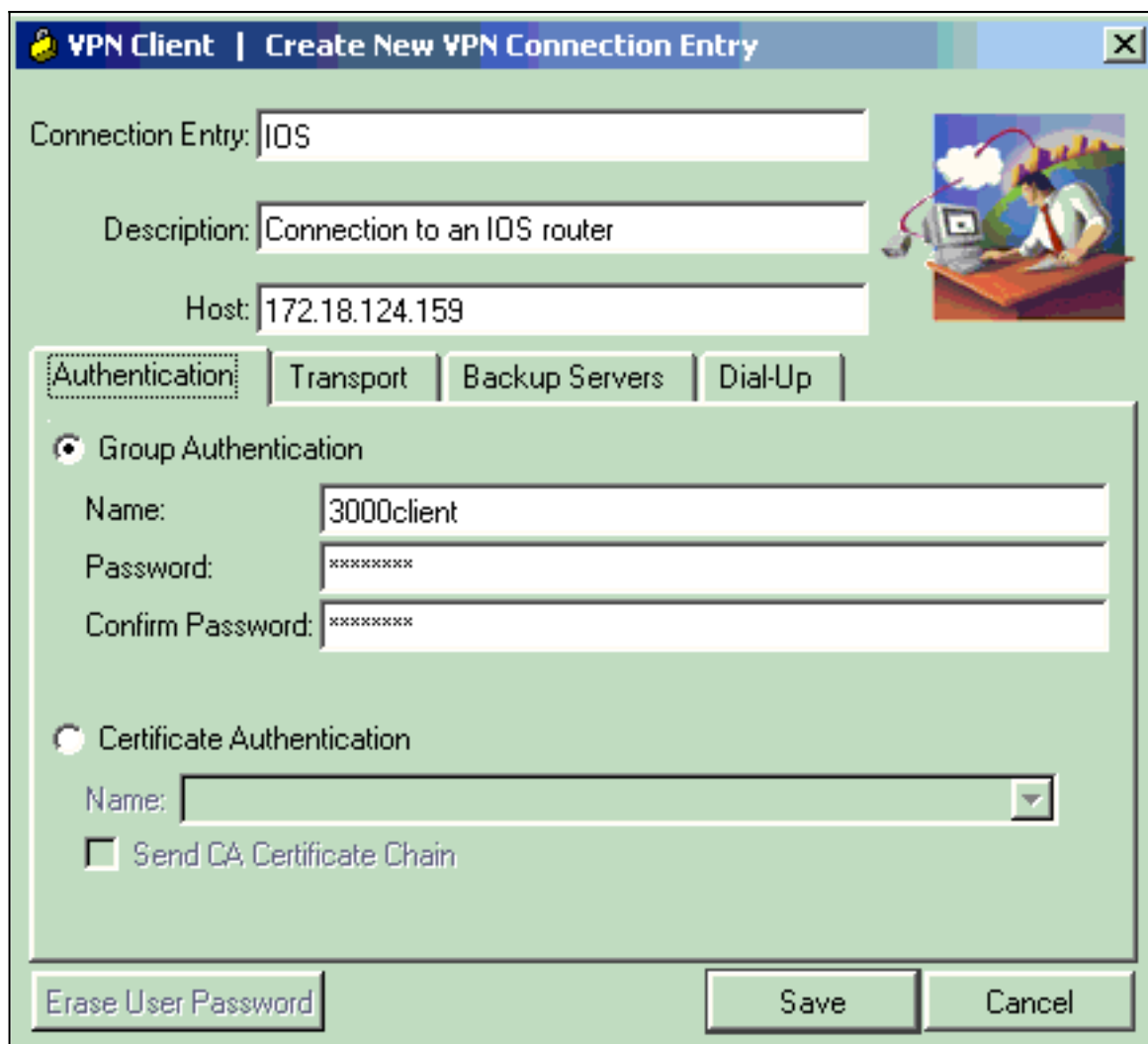
[Настройте клиент VPN 4. x](#)

Выполните эти действия для настройки Cisco VPN Client 4. x.

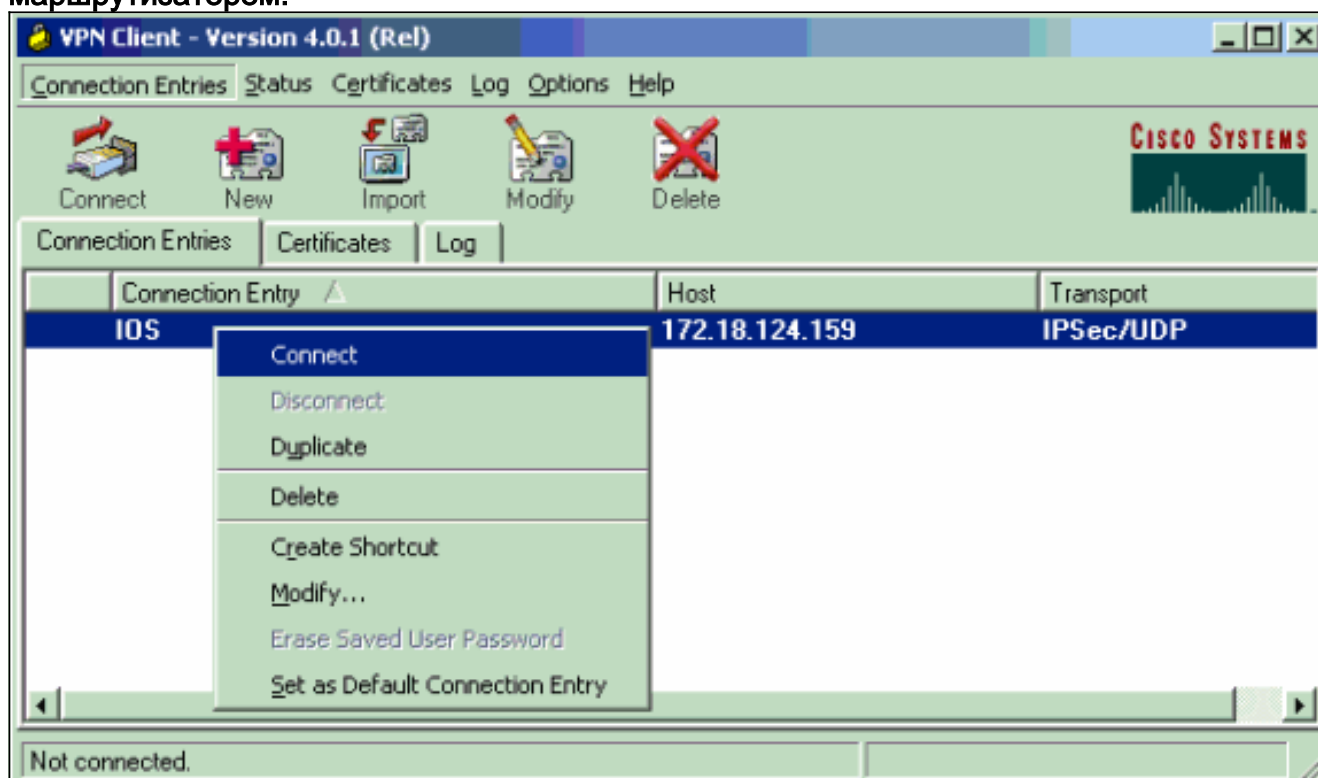
1. Запустите VPN Client, а затем нажмите кнопку New, чтобы создать новое соединение.



2. Введите необходимую информацию и по завершении нажмите кнопку "Сохранить".



- Щелкните правой кнопкой мыши на вновь созданном экземпляре соединения, а затем выберите пункт меню **Connect** для установки соединения с маршрутизатором.



- Во время согласований по протоколу IPsec будет предложено ввести имя



пользователя и пароль.

5. В окне появятся сообщения "Negotiating security profiles" (Выполняется согласование профилей безопасности) и "Your link is now secure" (Безопасность канала обеспечена)."

Проверка

В данном разделе приводятся сведения о проверке правильности функционирования вышенастроенной конфигурации.

Некоторые команды **show** поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды **show**.

Виртуальная частная сеть Cisco 2611

```
vpn2611#show crypto isakmp sa dst src state conn-id slot 172.18.124.159 172.18.124.199 QM_IDLE 5
0 !--- For the LAN-to-LAN tunnel peer. 172.18.124.159 64.102.55.142 QM_IDLE 6 0 !--- For the
Cisco Unity Client tunnel peer. vpn2611#show crypto ipsec sa interface: Ethernet0/0 Crypto map
tag: clientmap, local addr. 172.18.124.159 protected vrf: local ident (addr/mask/prot/port):
(10.10.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port):
(10.10.20.0/255.255.255.0/0/0) current_peer: 172.18.124.199:500 !--- For the LAN-to-LAN tunnel
peer. PERMIT, flags={origin_is_acl,} #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4 #pkts
decaps: 4, #pkts decrypt: 4, #pkts verify 4 #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.: 172.18.124.159, remote crypto endpt.: 172.18.124.199 path mtu 1500, media
mtu 1500 current outbound spi: 892741BC inbound esp sas: spi: 0x7B7B2015(2071666709) transform:
esp-3des esp-md5-hmac , in use settings = {Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto
map: clientmap sa timing: remaining key lifetime (k/sec): (4607999/1182) IV size: 8 bytes replay
detection support: Y inbound ah sas: inbound pcg sas: outbound ESP sas: spi:
```

```

0x892741BC(2301051324) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2001, flow_id: 2, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4607999/1182) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound PCP sas:
protected vrf: local ident (addr/mask/prot/port): (172.18.124.159/255.255.255.255/0/0) remote
ident (addr/mask/prot/port): (14.1.1.106/255.255.255.255/0/0) current_peer: 64.102.55.142:500 !-
-- For the Cisco Unity Client tunnel peer. 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.: 172.18.124.159, remote crypto endpt.:
64.102.55.142 path mtu 1500, media mtu 1500 current outbound spi: 81F39EFA inbound ESP sas: spi:
0xC4483102(3293065474) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2002, flow_id: 3, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4608000/3484) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound PCP sas:
outbound ESP sas: spi: 0x81F39EFA(2180226810) transform: esp-3des esp-md5-hmac , in use settings
={Tunnel, } slot: 0, conn id: 2003, flow_id: 4, crypto map: clientmap sa timing: remaining key
lifetime (k/sec): (4608000/3484) IV size: 8 bytes replay detection support: Y outbound ah sas:
outbound PCP sas: protected vrf: local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote
ident (addr/mask/prot/port): (14.1.1.106/255.255.255.255/0/0) current_peer: 64.102.55.142:500 !-
-- For the Cisco Unity Client tunnel peer. PERMIT, flags={} #pkts encaps: 4, #pkts encrypt: 4,
#pkts digest 4 #pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20 #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.: 172.18.124.159, remote crypto endpt.:
64.102.55.142 path mtu 1500, media mtu 1500 current outbound spi: B7F84138 inbound ESP sas: spi:
0x5209917C(1376358780) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2004, flow_id: 5, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4607998/3474) IV size: 8 bytes replay detection support: Y spi: 0xDE6C99C0(3731659200)
transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2006, flow_id:
7, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4607998/3493) IV size: 8
bytes replay detection support: Y inbound ah sas: inbound PCP sas: outbound ESP sas: spi:
0x58886878(1485334648) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2005, flow_id: 6, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4608000/3474) IV size: 8 bytes replay detection support: Y spi: 0xB7F84138(3086500152)
transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2007, flow_id:
8, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4607999/3486) IV size: 8
bytes replay detection support: Y outbound ah sas: outbound PCP sas: vpn2611#show crypto engine
connection active ID Interface IP-Address State Algorithm Encrypt Decrypt 5 Ethernet0/0
172.18.124.159 set HMAC_MD5+DES_56_CB 0 0 6 Ethernet0/0 172.18.124.159 set HMAC_SHA+3DES_56_C 0
0 2000 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 4 2001 Ethernet0/0 172.18.124.159 set
HMAC_MD5+3DES_56_C 4 0 2002 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 0 2003
Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 0 2004 Ethernet0/0 172.18.124.159 set
HMAC_MD5+3DES_56_C 0 9 2005 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 0 2006
Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 79 2007 Ethernet0/0 172.18.124.159 set
HMAC_MD5+3DES_56_C 4 0 vpn2611#

```

Cisco VPN 3640

```

vpn3640#show crypto isakmp sa DST src state conn-id slot 172.18.124.159 172.18.124.199 QM_IDLE 4
0 !--- For the LAN-to-LAN tunnel peer. vpn3640#show crypto ipsec sa interface: Ethernet0/0
Crypto map tag: mymap, local addr. 172.18.124.199 protected vrf: local ident
(addr/mask/prot/port): (10.10.20.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port):
(10.10.10.0/255.255.255.0/0/0) current_peer: 172.18.124.159:500 !--- For the LAN-to-LAN tunnel
peer. PERMIT, flags={origin_is_acl,} #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4 #pkts
decaps: 4, #pkts decrypt: 4, #pkts verify 4 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0 #send errors 11, #recv errors
0 local crypto endpt.: 172.18.124.199, remote crypto endpt.: 172.18.124.159 path mtu 1500, media
mtu 1500 current outbound spi: 7B7B2015 inbound ESP sas: spi: 0x892741BC(2301051324) transform:
esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 940, flow_id: 1, crypto
map: mymap sa timing: remaining key lifetime (k/sec): (4607998/1237) IV size: 8 bytes replay
detection support: Y inbound ah sas: inbound PCP sas: outbound ESP sas: spi:
0x7B7B2015(2071666709) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 941, flow_id: 2, crypto map: mymap sa timing: remaining key lifetime (k/sec):
(4607999/1237) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound PCP sas:
vpn3640# show crypto engine connection active ID Interface IP-Address State Algorithm Encrypt
Decrypt 4 <none> <none> set HMAC_MD5+DES_56_CB 0 0 940 Ethernet0/0 172.18.124.199 set

```


[Проверьте порядковые номера криптокарты](#)

Если статические и динамические узлы настроены на той же криптокарте, заказ элементов криптокарты очень важен. Порядковый номер записи динамической криптокарты **должен быть** выше, чем все другие записи статической криптокарты. Если статические записи пронумерованы выше, чем динамическая запись, соединения с теми узлами сбой.

Вот пример должным образом пронумерованной криптокарты, которая содержит статическую запись и динамическую запись. Обратите внимание на то, что динамическая запись имеет самый высокий порядковый номер, и команду покинули добавить дополнительные статические записи:

```
crypto dynamic-map dynmap 10
set transform-set myset
crypto map clientmap 1 ipsec-isakmp
set peer 172.18.124.199
set transform-set myset
match address 100
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
```

[Устранение неполадок](#)

В данном разделе содержатся сведения, помогающие при поиске и устранении неполадок конфигурации.

[Команды для устранения неполадок](#)

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

Примечание: См. [раздел Важные сведения о командах отладки](#) перед запуском команд отладки.

- **debug crypto ipsec**– показывает события IPSec. Вид «по» этой команды отключает вывод отладочных данных.
- **debug crypto isakmp** – отображает сообщения о событиях IKE. Вид «по» этой команды отключает вывод отладочных данных.
- **debug crypto engine**, который принадлежит ядру шифрования, такой как тогда, когда программное обеспечение Cisco IOS выполняет шифрование или операции по расшифровке.

[Дополнительные сведения](#)

- [Страница поддержки IPsec Negotiation/IKE](#)
- [Cisco Systems – техническая поддержка и документация](#)