Динамический Туннель IPSec Между Статически Обращенным ASA и Динамично Обращенным маршрутизатором Cisco IOS, который использует Пример конфигурации CCP

Содержание

Введение

Этот документ предоставляет пример конфигурации для того, как позволить Устройству безопасности PIX/ASA принять динамические подключения IPsec от маршрутизатора Cisco IOS®. В этом сценарии туннель IPSec устанавливается только в том случае, когда туннель инициируется со стороны Маршрутизатора. Динамическая конфигурация IPSec может не позволить устройству ASA инициировать VPN-туннель.

Эта конфигурация позволяет устройству защиты PIX создавать динамический IPsec-туннель для соединения локальных сетей (LAN–LAN, L2L) с удаленным маршрутизатором VPN. Этот маршрутизатор динамично получает свой внешний открытый IP - адрес от его интернет-провайдера. Этот механизм динамического выделения IP-адресов от поставщика услуг реализуется протоколом DHCP. При этом IP-адреса, переставшие быть востребованными для хостов, можно использовать повторно.

Конфигурация на маршрутизаторе реализована с использованием Cisco Configuration

Professional (CCP). CCP на основе GUI программное средство управления устройствами, которое позволяет вам настраивать Маршрутизаторы на основе IOS Cisco. См. Базовую настройку маршрутизатора Использование Cisco Configuration Professional для получения дополнительной информации о том, как настроить маршрутизатор с CCP.

См. Узел к VPN Узла (L2L) с ASA для большего количества inormation и примеров конфигурации на установлении Туннеля IPSec, которые используют ASA и маршрутизаторы Cisco IOS.

См. Узел к VPN Узла (L2L) с IOS для получения дополнительной информации и примером конфигурации на динамическом установлении Туннеля IPSec с использованием PIX и маршрутизатора Cisco IOS.

Предварительные условия

Требования

Прежде чем вы будете делать попытку этой конфигурации, будете гарантировать, что и ASA и маршрутизатор имеют интернет-соединение для установления Туннеля IPSec.

Используемые компоненты

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

- Cisco IOS Router1812, который выполняет Cisco IOS Software Release 12.4
- Выпуск ПО Cisco ASA 5510 8.0.3

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

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

В этом сценарии 192.168.100.0 сети находятся позади ASA, и 192.168.200.0 сети находятся позади маршрутизатора Cisco IOS. Предполагается, что маршрутизатор получает свой общий адрес через DHCP от его интернет-провайдера. Поскольку это излагает проблему в конфигурации статического однорангового узла на конце ASA, необходимо приблизиться к способу динамического крипта - настройки установить туннель от узла к узлу между ASA и маршрутизатором Cisco IOS.

Интернет-пользователи в конце ASA преобразованы в IP-адрес его внешнего интерфейса. Предполагается, что NAT не настроен на конце маршрутизатора Cisco IOS.

Теперь это основные шаги, которые будут настроены на конце ASA, для установления динамического туннеля:

1. Связанная конфигурация ISAKMP фазы 1
2. Туземная конфигурация освобождения
3. Конфигурация динамической криптокарты

Маршрутизатору Cisco IOS настроили статическую криптокарту, потому что ASA, как предполагается, имеет статический открытый IP - адрес. Теперь это - список основных шагов, которые будут настроены на конце маршрутизатора Cisco IOS для установления динамического Туннеля IPSec.

1. Связанная конфигурация ISAKMP фазы 1
2. Связанная конфигурация статической криптокарты

Эти шаги описаны подробно в этих конфигурациях.

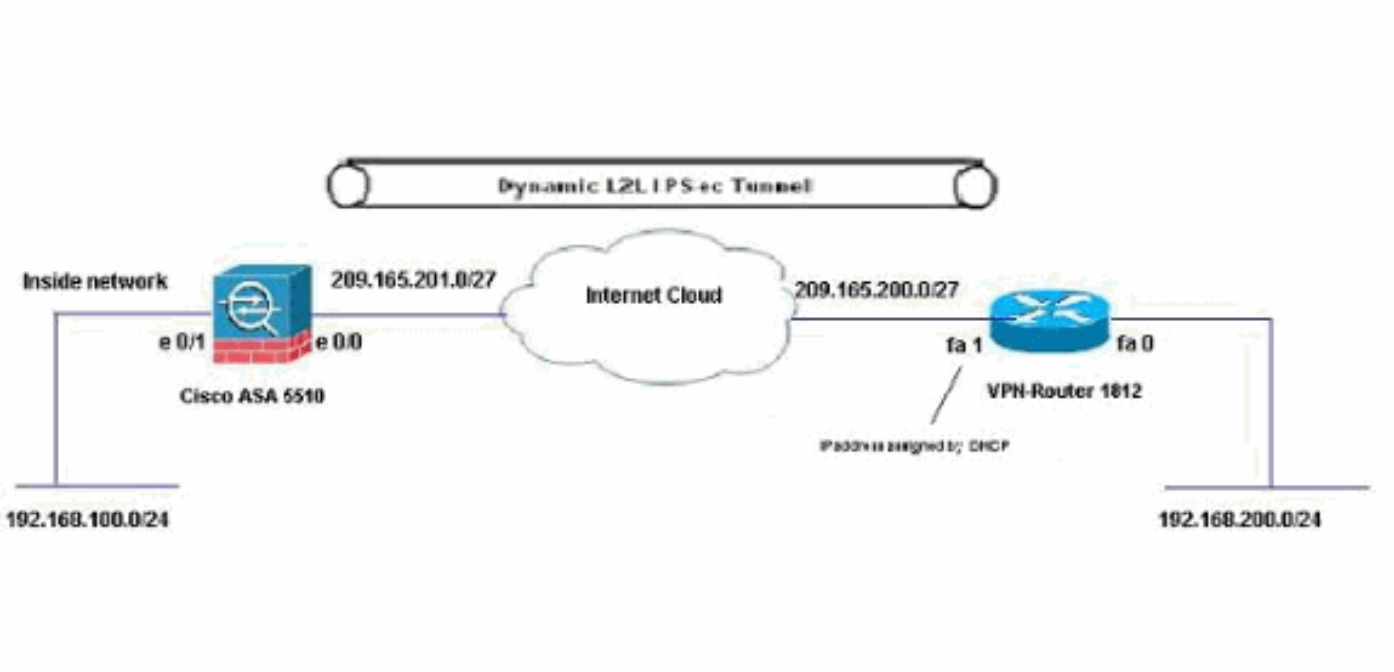
Настройка

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

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

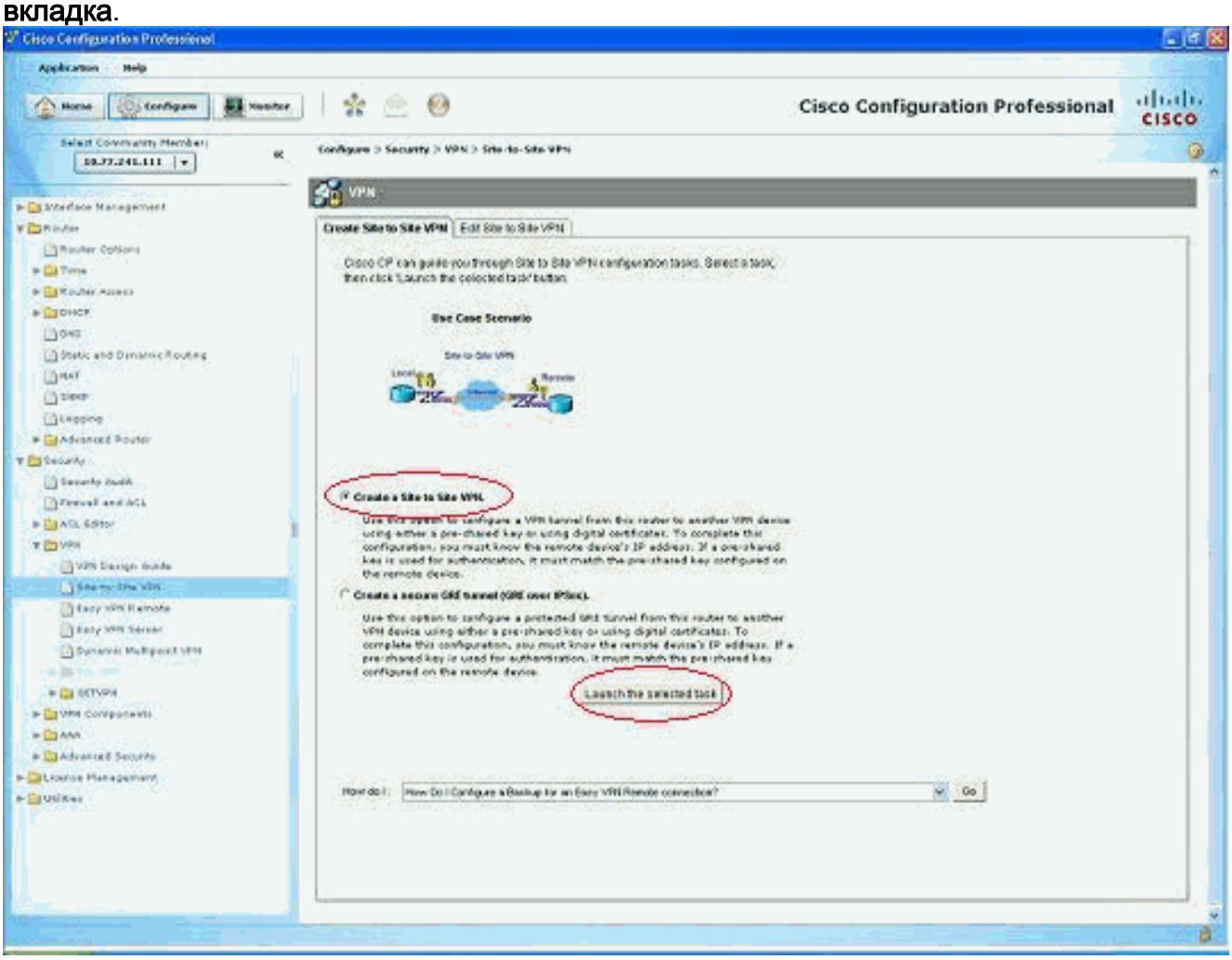
В настоящем документе используется следующая схема сети:



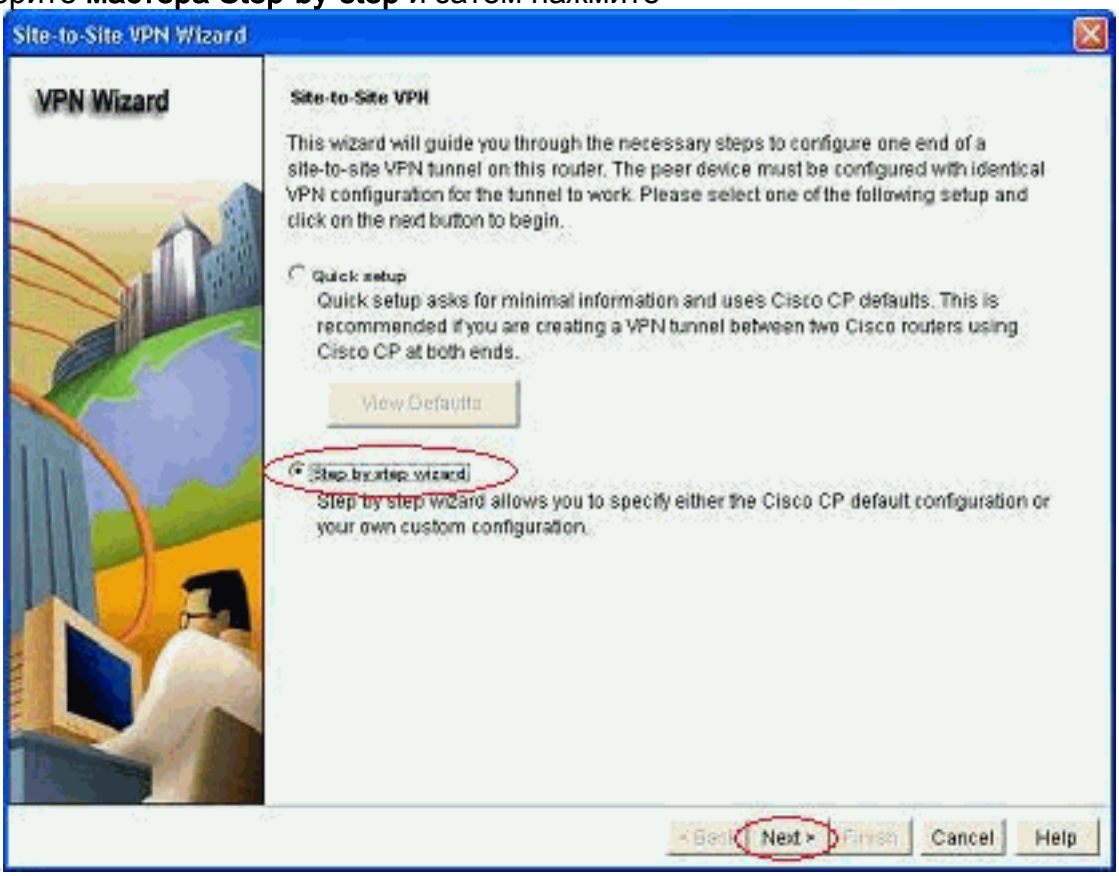
Конфигурации

Это - конфигурация IPSec VPN на Маршрутизаторе с поддержкой VPN с CCP. Выполните следующие действия:

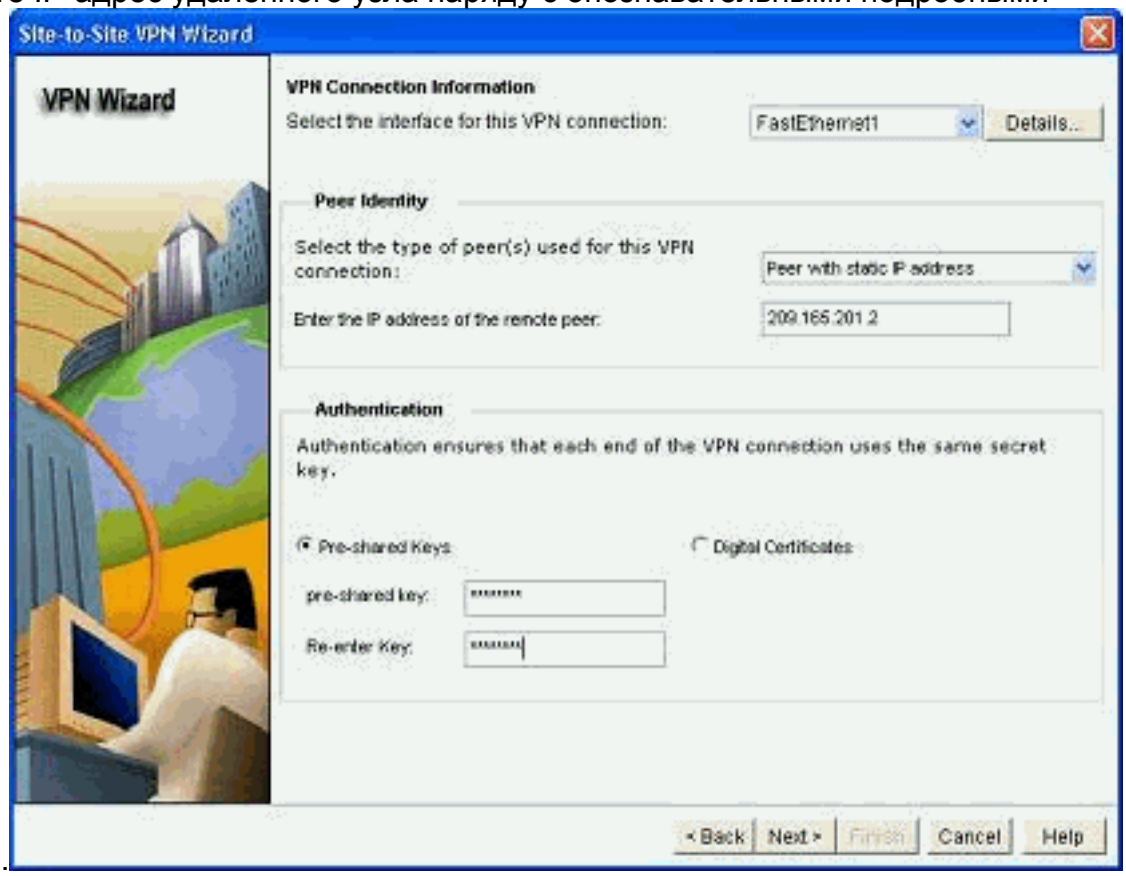
1. Откройте приложение CCP и выберите**> Security Configure> VPN> Узел к VPN Узла**. Нажмите **Launch выбранная вкладка**.



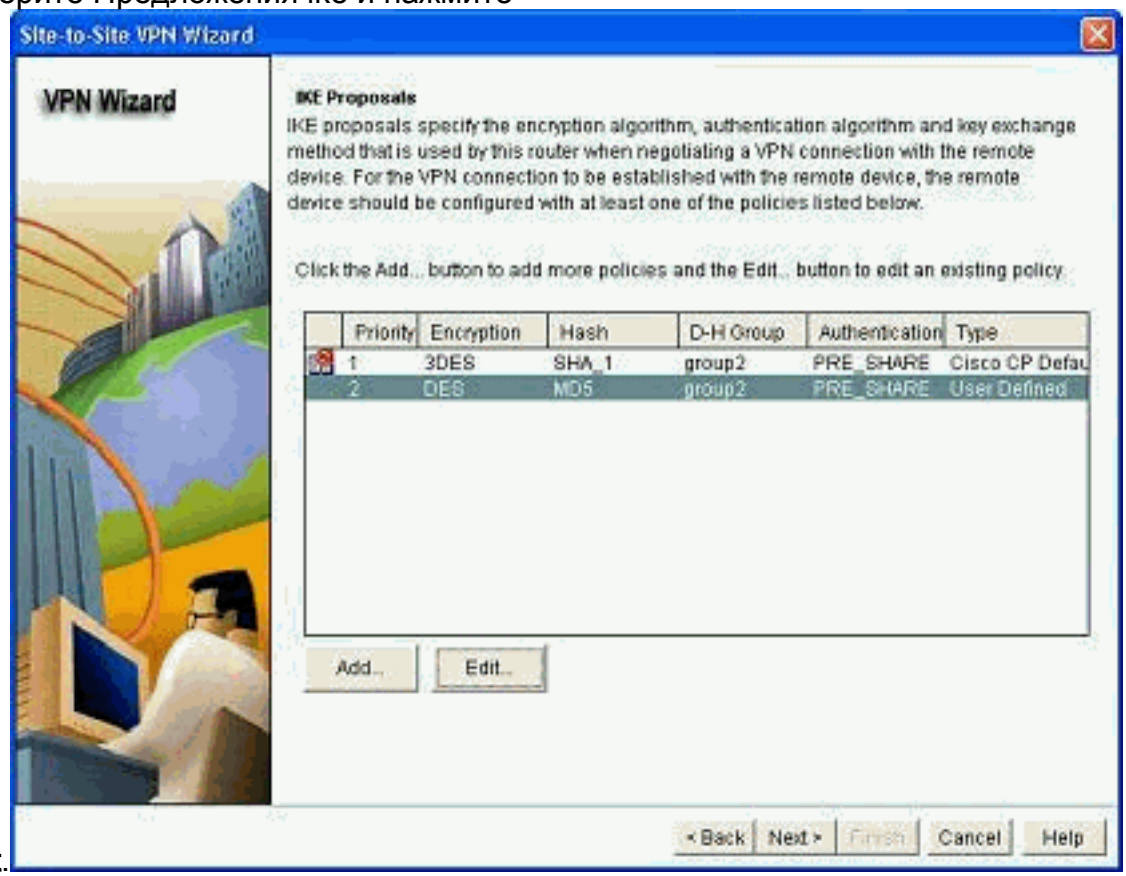
2. Выберите **мастера Step-by-step** и затем нажмите **Next**.



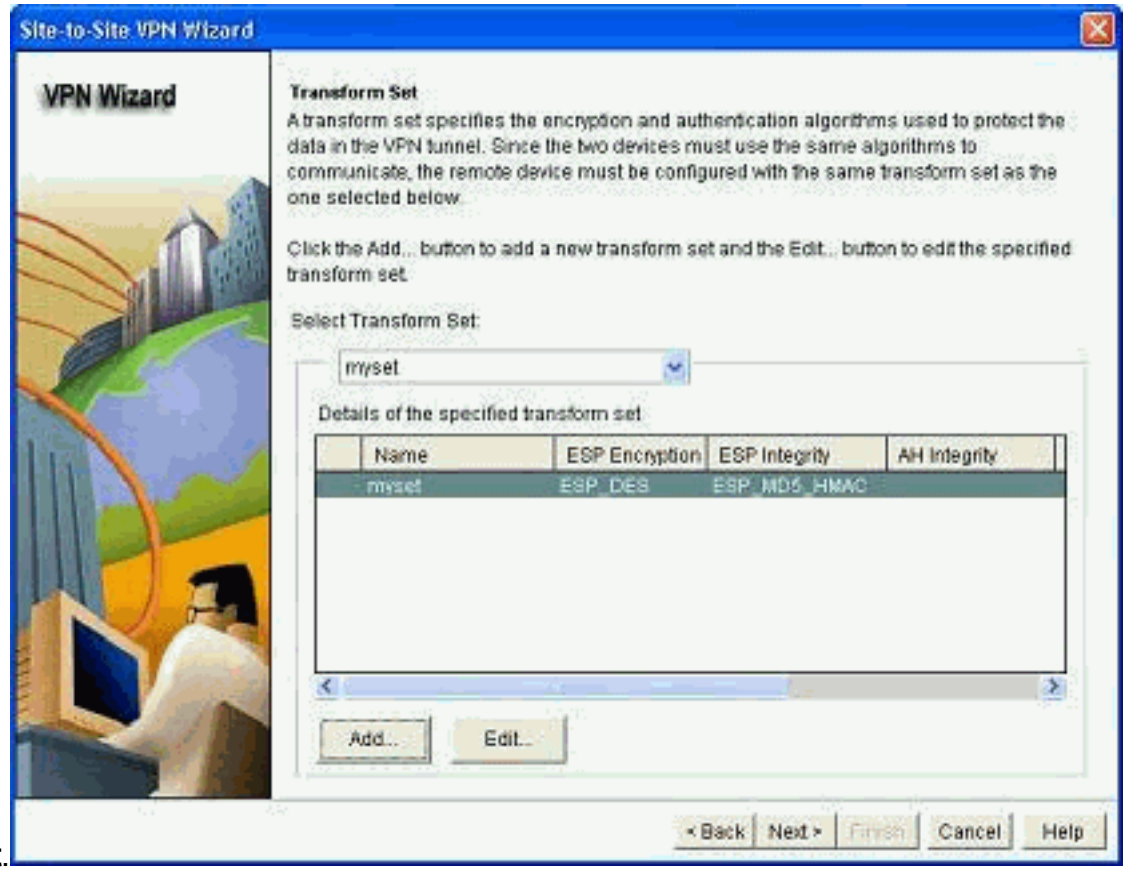
3. Заполните IP-адрес удаленного узла наряду с опознавательными подробными данными.



4. Выберите Предложения ike и нажмите **Next**.

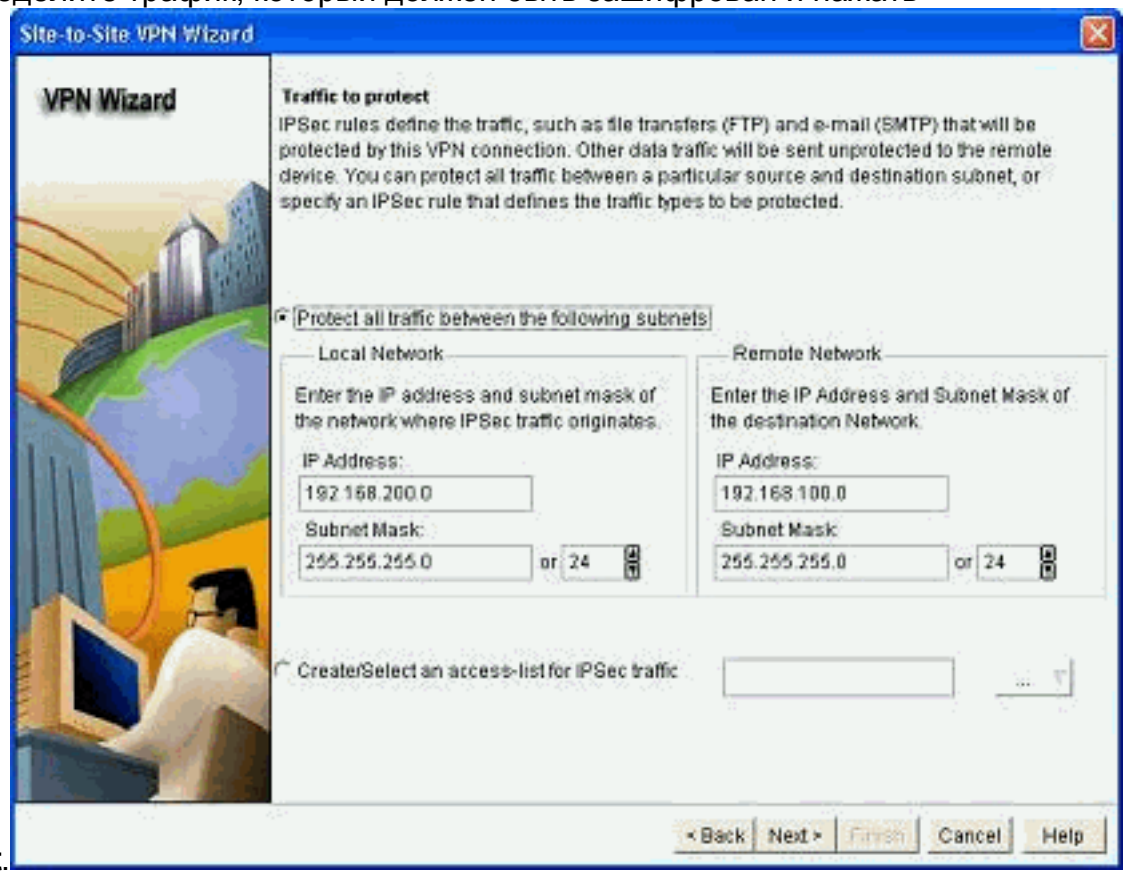


5. Определите подробные данные transform-set и нажмите



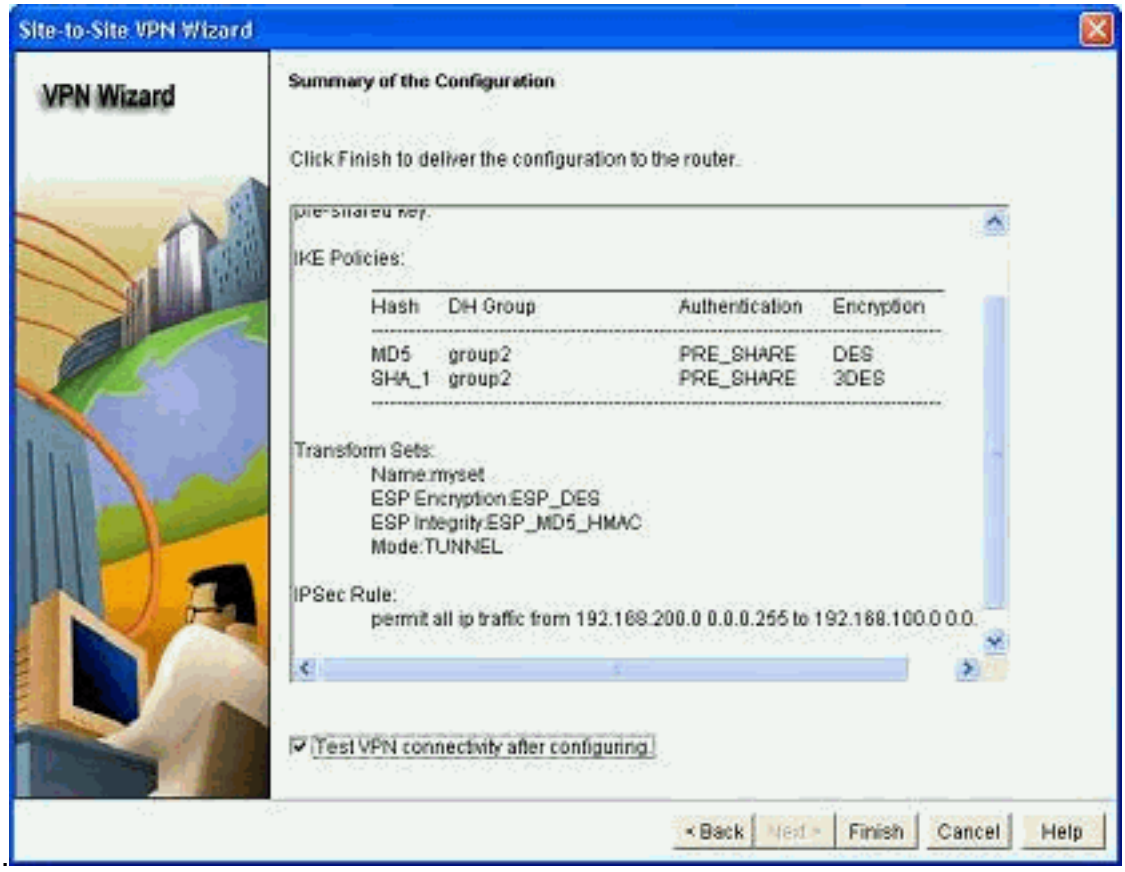
Next.

6. Определите трафик, который должен быть зашифрован и нажать



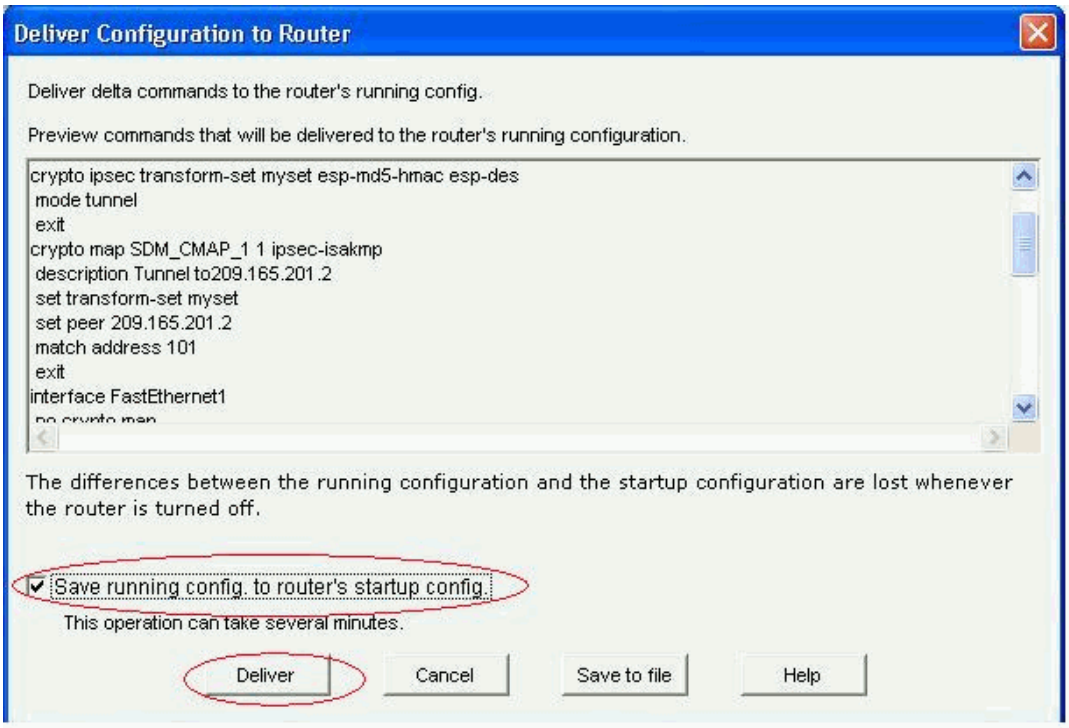
Next.

7. Проверьте сводку крипто-Конфигурации IPSec и нажмите

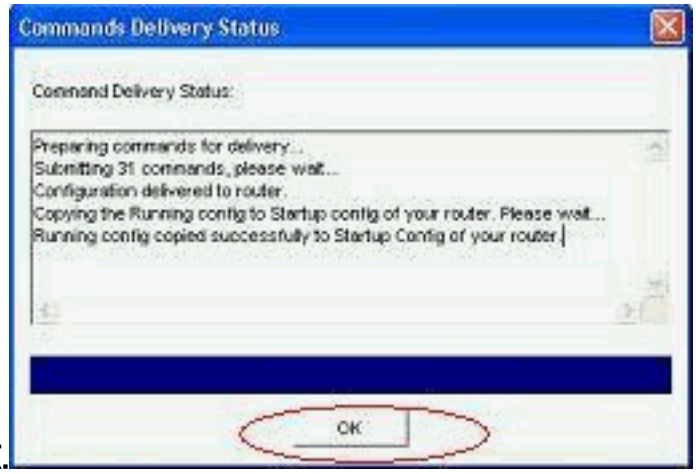


Finish.

8. Нажмите **Deliver** для передачи конфигурации к Маршрутизатору с поддержкой VPN.



9. **Нажмите кнопку OK.**



Конфигурация интерфейса командой строки CLI

- Cisco ASA
- Маршрутизатор с поддержкой VPN

Cisco ASA

```
ciscoasa(config)#show run : Saved : ASA Version 8.0(3) !
hostname ciscoasa enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif outside
security-level 0 ip address 209.165.201.2
255.255.255.224 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 192.168.100.1
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive !--- Output suppressed access-list
nonat extended permit ip 192.168.100.0 255.255.255.0
192.168.200.0 255.255.255.0 no pager mtu outside 1500
mtu inside 1500 icmp unreachable rate-limit 1 burst-size
1 asdm image disk0:/asdm-613.bin no asdm history enable
arp timeout 14400 ! !--- Define the nat-translation for
Internet users global (outside) 1 interface nat (inside)
1 192.168.100.0 255.255.255.0 ! ! !--- Define the nat-
exemption policy for VPN traffic nat (inside) 0 access-
list nonat ! route outside 0.0.0.0 0.0.0.0 209.165.201.1
1 ! timeout xlate 3:00:00 timeout conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc
0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite
0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00
absolute dynamic-access-policy-record DfltAccessPolicy
no snmp-server location no snmp-server contact snmp-
server enable traps snmp authentication linkup linkdown
coldstart ! !--- Configure the IPsec transform-set
crypto ipsec transform-set myset esp-des esp-md5-hmac !
! !--- Configure the dynamic crypto map crypto dynamic-
map mymap 1 set transform-set myset crypto dynamic-map
mymap 1 set reverse-route crypto map dyn-map 10 IPSec-
isakmp dynamic mymap crypto map dyn-map interface
outside ! !--- Configure the phase I ISAKMP policy
crypto isakmp policy 10 authentication pre-share
encryption des hash md5 group 2 lifetime 86400 ! ! !---
Configure the default L2L tunnel group parameters
tunnel-group DefaultL2LGroup IPSec-attributes pre-
shared-key * ! class-map inspection_default match
```

```
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa(config)#
```

CCP создает эту конфигурацию на Маршрутизаторе с поддержкой VPN.

Маршрутизатор с поддержкой VPN

```
VPN-Router#show run Building configuration... ! version
12.4 service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname VPN-Router ! ! username cisco
privilege 15 secret 5 $1$UQxM$WvwDZbfDhK3wS26C9xYns/
username test12 privilege 15 secret 5
$1$LC0U$ex3tp4hM8CYD.HJSRDfQO1 ! ! !--- Output
suppressed no aaa new-model ip subnet-zero ! ip cef !
crypto isakmp enable outside ! crypto isakmp policy 1
encrypt 3des authentication pre-share group 2 ! crypto
isakmp policy 2 hash md5 authentication pre-share group
2 ! ! crypto isakmp key cisco123 address 209.165.201.2 !
! crypto ipsec transform-set myset esp-des esp-md5-hmac
! ! crypto map SDM_CMAP_1 1 IPSec-isakmp description
Tunnel to209.165.201.2 set peer 209.165.201.2 set
transform-set myset match address 101 ! ! ! interface
BRI0 no ip address shutdown ! interface Dot11Radio0 no
ip address shutdown speed basic-1.0 basic-2.0 basic-5.5
6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root ! interface Dot11Radio1 no ip address
shutdown speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0
36.0 48.0 54.0 station-role root ! interface
FastEthernet0 ip address 192.168.200.1 255.255.255.0
duplex auto speed auto ! interface FastEthernet1 ip
address dhcp duplex auto speed auto crypto map
SDM_CMAP_1 ! interface FastEthernet2 no ip address
shutdown ! interface FastEthernet3 no ip address
shutdown ! interface FastEthernet4 no ip address
shutdown ! interface FastEthernet5 no ip address
shutdown ! interface FastEthernet6 no ip address
shutdown ! interface FastEthernet7 no ip address
shutdown ! interface FastEthernet8 no ip address
shutdown ! interface FastEthernet9 no ip address
shutdown ! interface Vlan1 no ip address ! ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1 ! ! !--- Output
suppressed ! ip http server ip http authentication local
ip http secure-server ! access-list 100 permit ip
0.0.0.0 255.255.255.0 0.0.0.0 255.255.255.0 access-list
101 remark CCP_ACL Category=4 access-list 101 remark
IPSEC Rule access-list 101 permit ip 192.168.200.0
0.0.0.255 192.168.100.0 0.0.0.255 ! ! ! ! control-plane
! ! line con 0 line aux 0 line vty 0 4 privilege level
15 login local transport input telnet ssh line vty 5 15
privilege level 15 login local transport input telnet
ssh ! no scheduler allocate end
```

Проверка

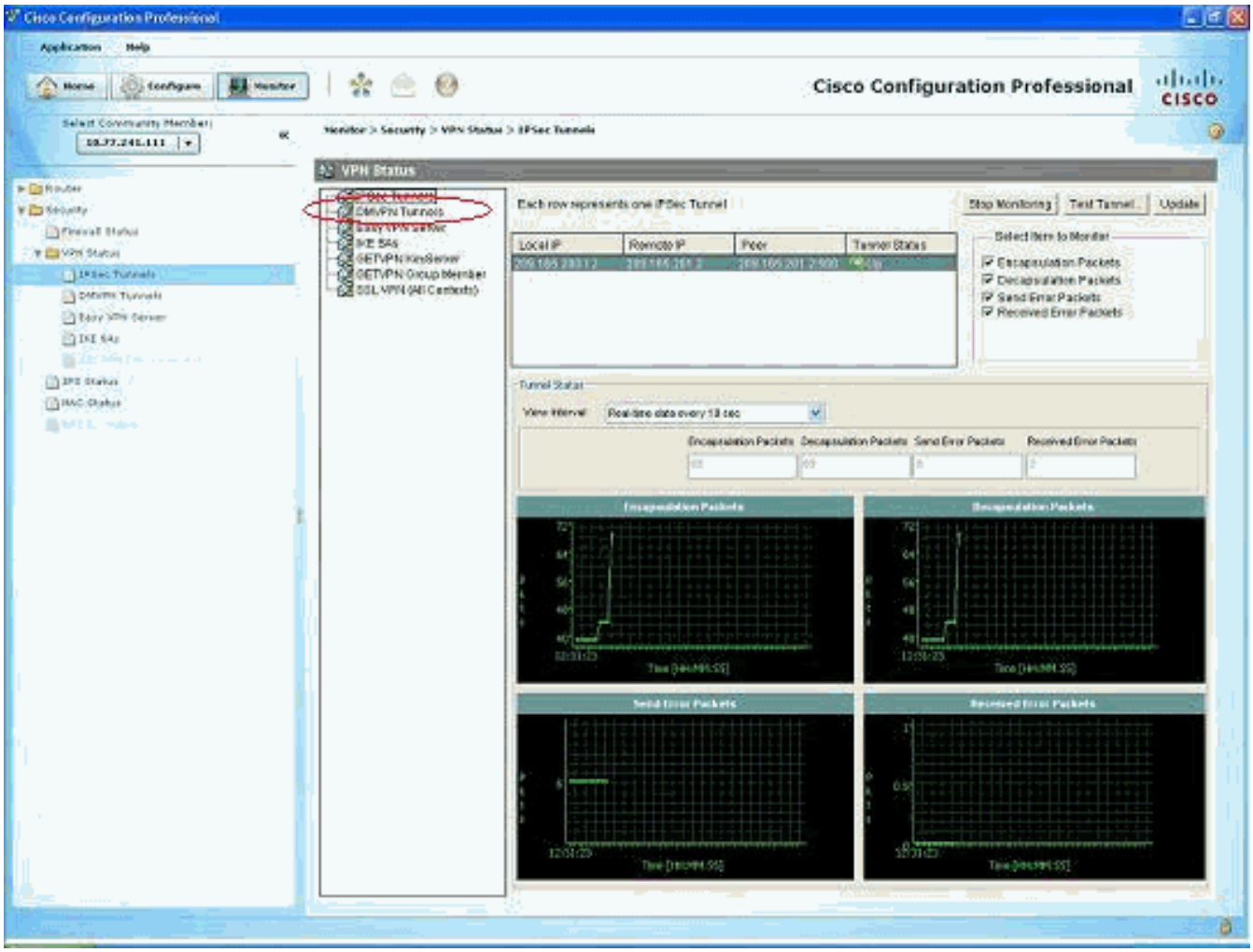
Этот раздел позволяет убедиться, что конфигурация работает правильно.

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

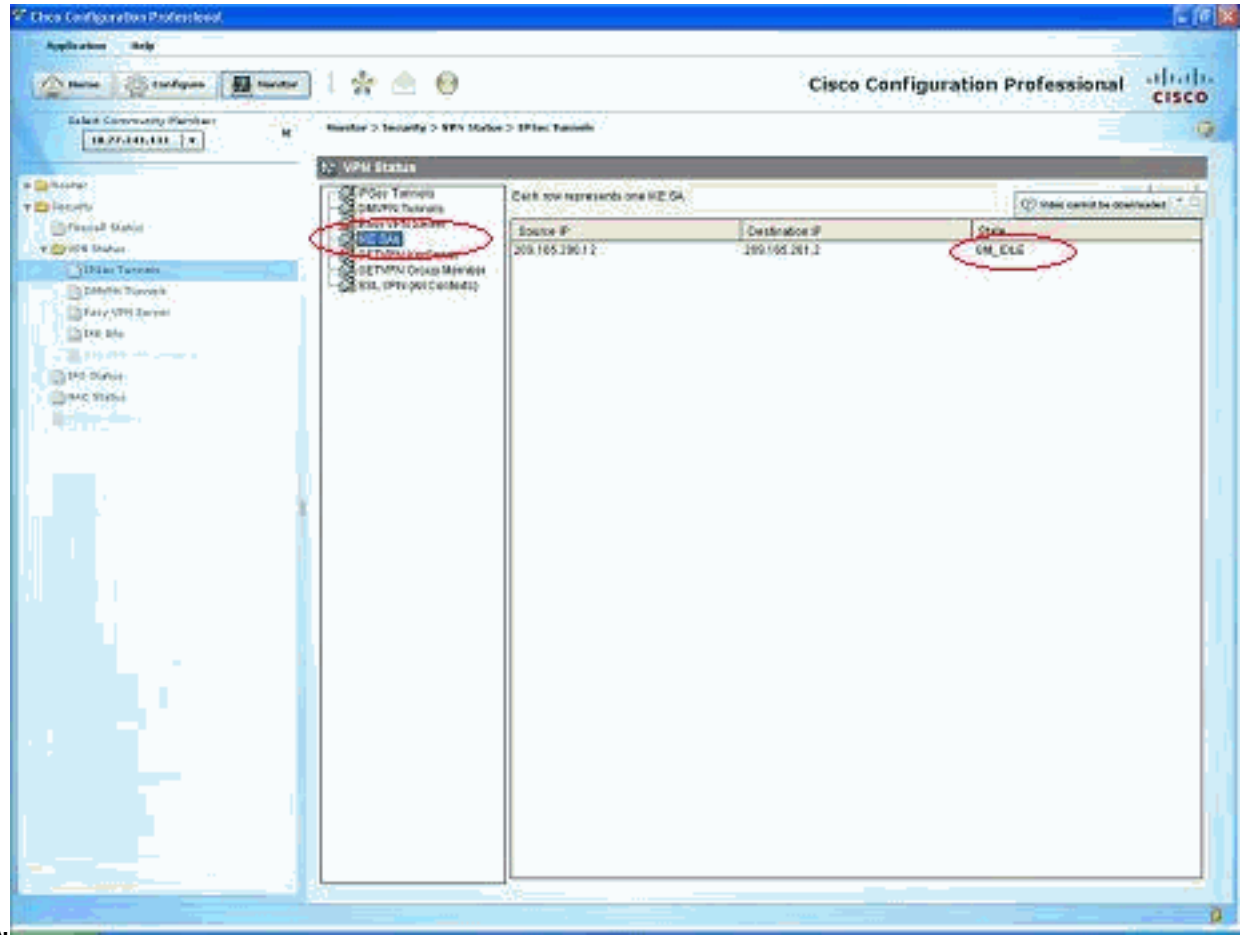
- Проверка параметров туннеля через CCP
- Проверка статуса туннеля через CLI ASA
- Проверка параметров туннеля через CLI маршрутизатора

Проверьте параметры туннеля через CCP

- Контролируйте трафик проходит через Туннель IPSec.



- Контролируйте статус фазы I ISAKMP

SA. 

Проверьте статус туннеля через CLI ASA

- Проверьте статус фазы I ISAKMP SA.`ciscoasa#`**`show crypto isakmp sa`** `Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 209.165.200.12 Type : L2L Role :` **`responder`** `Rekey : no State :` **`MM_ACTIVE`** `ciscoasa#`

  Примечание: Наблюдайте, что Роль респондент, который сообщает, что инициатором этого туннеля является с другой стороны, например, Маршрутизатор с поддержкой VPN.
- Проверьте параметры КОНТЕКСТА БЕЗОПАСНОСТИ IPSEC этапа 2.`ciscoasa#`**`show crypto ipsec sa`** `interface: outside Crypto map tag: mymap, seq num: 1, local addr: 209.165.201.2` **`local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)`** `current_peer: 209.165.200.12` **`#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29 #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29`** `#pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 209.165.201.2, remote crypto endpt.: 209.165.200.12 path mtu 1500, IPSec overhead 58, media mtu 1500 current outbound spi: E7B37960 inbound esp sas: spi: 0xABB49C64 (2880740452) transform: esp-des esp-md5-hmac none in use settings ={L2L, Tunnel, } slot: 0, conn_id: 4096, crypto-map: mymap sa timing: remaining key lifetime (kB/sec): (4274997/3498) IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xE7B37960 (3887298912) transform: esp-des esp-md5-hmac none in use settings ={L2L, Tunnel, } slot: 0, conn_id: 4096, crypto-map: mymap sa timing: remaining key lifetime (kB/sec): (4274997/3498) IV size: 8 bytes replay detection support: Y`

Проверьте параметры туннеля через CLI маршрутизатора

- Проверьте статус фазы I ISAKMP SA.`VPN-Router#`**`show crypto isakmp sa`** `dst src state conn-id slot status 209.165.201.2 209.165.200.12` **`QM_IDLE`** `1 0` **`ACTIVE`**
- Проверьте параметры КОНТЕКСТА БЕЗОПАСНОСТИ IPSEC этапа 2.`VPN-Router#`**`show`**

```
crypto ipsec sa interface: FastEthernet1 Crypto map tag: SDM_CMAP_1, local addr
209.165.200.12 protected vrf: (none) local ident (addr/mask/prot/port):
(192.168.200.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port):
(192.168.100.0/255.255.255.0/0/0) current_peer 209.165.201.2 port 500 PERMIT,
flags={origin_is_acl,} #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39 #pkts decaps:
39, #pkts decrypt: 39, #pkts verify: 39 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 6, #recv errors 0 local crypto endpt.: 209.165.200.12, remote crypto endpt.:
209.165.201.2 path mtu 1500, ip mtu 1500 current outbound spi: 0xABB49C64(2880740452)
inbound esp sas: spi: 0xE7B37960(3887298912) transform: esp-des esp-md5-hmac , in use
settings ={Tunnel, } conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1 sa timing:
remaining key lifetime (k/sec): (4481818/3375) IV size: 8 bytes replay detection support: Y
Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0xABB49C64(2880740452) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } conn
id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1 sa timing: remaining key lifetime
(k/sec): (4481818/3371) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound
ah sas: outbound pcp sas:
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

- Разъединение существующих крипто-соединений.`ciscoasa#clear crypto ipsec sa ciscoasa#clear crypto isakmp sa VPN-Router#clear crypto isakmp`
- Используйте **команды отладки** для устренения проблем с VPN-туннелем.**Примечание:** Если вы включаете отладку, это может разрушить использование маршрутизатора, когда объединения нескольких локальных сетей испытывают условия высокой нагрузки. **Команды debug необходимо использовать с осторожностью.** Обычно рекомендуется использовать эти команды только под руководством представителя технической поддержки своего маршрутизатора при устранении конкретных проблем.`ciscoasa#debug crypto engine ciscoasa#debug crypto isakmp ciscoasa#debug crypto IPSec ciscoasa# VPN-Router#debug crypto engine Crypto Engine debugging is on VPN-Router#debug crypto isakmp Crypto ISAKMP debugging is on VPN-Router#debug crypto ipsec Crypto IPSEC debugging is on VPN-Router#`

См. debug crypto isakmp в Понимании и Использовании команд отладки для получения дополнительной информации об отладке commangs.

Дополнительные сведения

- Страница технической поддержки протоколов согласования IPSec и IKE
- Документация для операционного программного обеспечения устройства безопасности Cisco ASA
- Наиболее распространенные решения для устранения проблем IPSEC VPN
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация