Настройка L2TP по IPSec между межсетевым экраном PIX и Windows 2000 PC с помощью сертификатов

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Общие сведения
Настройка
Схема сети
Настройте Microsoft L2TP Client
Получите сертификаты для межсетевого экрана PIX
Конфигурация межсетевого экрана PIX
Проверка
Устранение неполадок
Команды для устранения неполадок
Пример результата отладки
Отладка, подходящая для регистрации в CA
Отладка, не подходящая для регистрации в CA
Дополнительные сведения

Введение

Протокол туннелирования уровня 2 (L2TP) через IPSec поддерживается на Выпуске ПО межсетевого экрана Cisco Secure PIX 6.x или позже. Пользователи, которые выполняют Windows 2000, могут использовать собственного клиента IPSec и клиента L2TP для установления туннеля L2TP к Межсетевому экрану PIX. Трафики через туннель L2TP зашифрованы Сопоставлениями безопасности IPSec (SA).

Примечание: Вы не можете использовать Клиента IPSEC Windows 2000 L2TP чтобы для Telnet к PIX.

Примечание: Разделенное туннелирование не доступно с L2TP на PIX.

Для настройки L2TP через IPsec от удаленного Microsoft Windows 2000/2003, и клиенты XP к офису корпорации Устройства безопасности PIX/ASA с помощью предварительных общих ключей с сервером RADIUS Интернет-сервиса проверки подлинности (IAS) Microsoft Windows 2003 года для проверки подлинности пользователя, обратитесь к L2TP По IPsec

Между Windows 2000/XP PC и Использованием примера конфигурации PIX/ASA 7.2 Предварительного общего ключа.

Для настройки L2TP через IP Security (IPsec) от удаленных клиентов Microsoft Windows 2000 и XP в корпоративный сайт с помощью зашифрованного метода см. Конфигурация L2TP через IPsec от клиента Windows 2000 или XP в концентратор Cisco VPN 3000 с использованием общих ключей.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе применяются к этим версиям программного и аппаратного обеспечения:

- Выпуск 6.3.3 программного обеспечения PIX
- Windows 2000 с или без SP2 (См. Q276360 Совета от Microsoft для получения информации о SP1.)

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

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

Поддержка сертификата в версиях Cisco Secure PIX 6.x или позже включает Балтимор, Microsoft, VeriSign, и Поручите серверы. В настоящее время PIX не принимает запросы L2TP без Защиты IPsec.

Данный пример показывает, как настроить Межсетевой экран PIX для сценария, упомянутого ранее в этом документе. Аутентификация Протокола IKE использует **команду rsa-sig** (сертификаты). В данном примере аутентификация сделана сервером RADIUS.

Параметры используемые в меньшей степени для зашифрованных клиентских соединений к PIX перечислены в Оборудовании CISCO и Клиентах VPN, Поддерживающих IPSec/PPTP/L2TP.

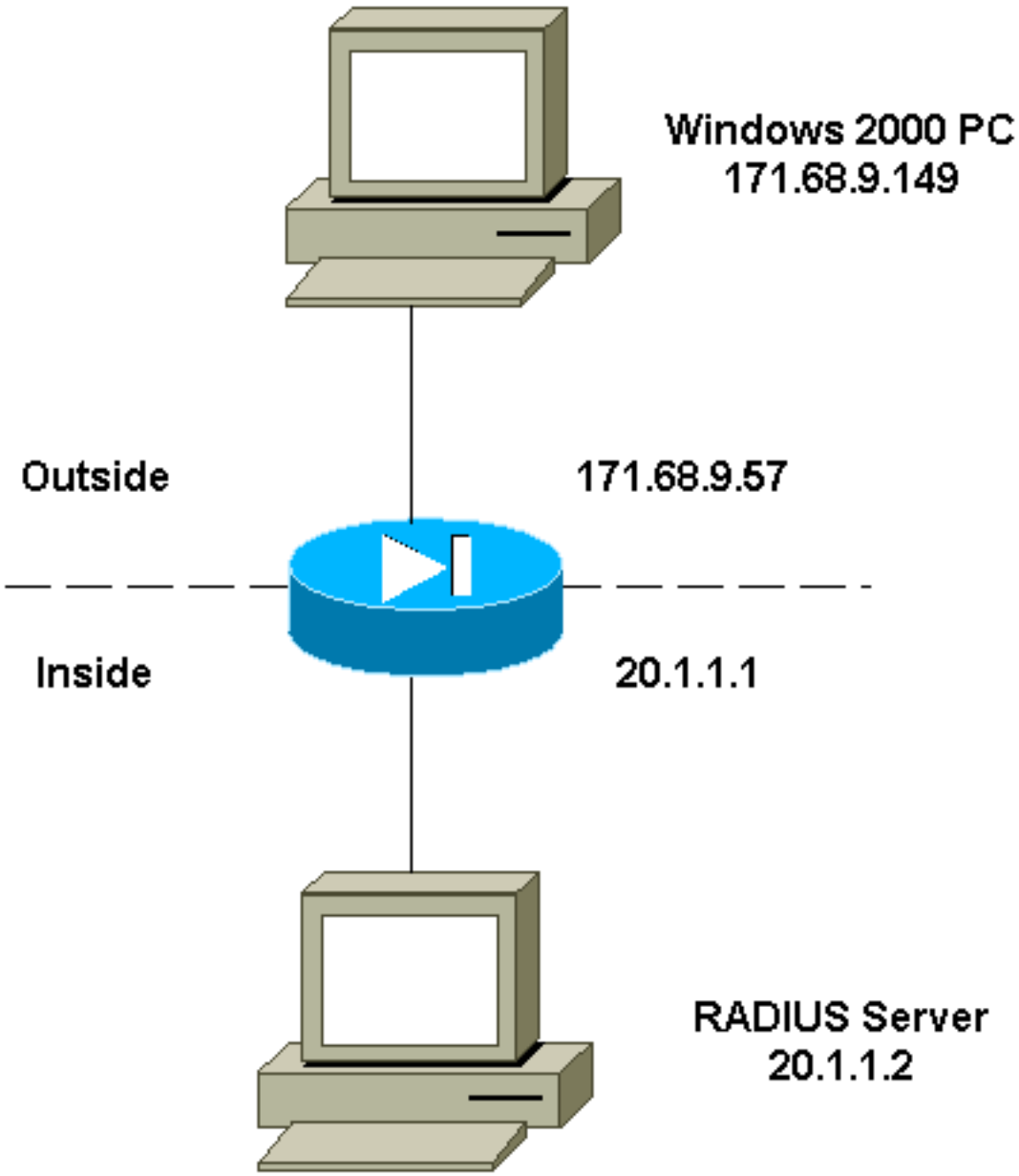
Настройка

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:



Настройте Microsoft L2TP Client

Информация о том, как настроить клиента Microsoft L2TP, найдена в Пошаговых инструкциях Microsoft к протоколу IPSEC (Internet Protocol Security) .

Как обращено внимание в пошаговых инструкциях, на которые ссылаются, от Microsoft, поддержки клиентов много протестированных серверов центра сертификации (CA). Информация о том, как установить Microsoft CA, найдена в Пошаговых инструкциях Microsoft к Устанавливанию Центра сертификации .

Получите сертификаты для межсетевого экрана PIX

См. Примеры конфигурации CA для подробных данных о том, как настроить PIX для совместимости с сертификатами от VeriSign, Поручите, Балтимор и Microsoft.

Конфигурация межсетевого экрана PIX

В данном документе используется следующая конфигурация.

Сетевой экран PIX

```
PIX Version 6.3(3)nameif ethernet0 outside
security0nameif ethernet1 inside security100enable
password 8Ry2YjIyt7RRXU24 encryptedpasswd
2KFQnbNIdI.2KYOU encryptedhostname PIX-506-2domain-name
sjvpn.comfixup protocol ftp 21fixup protocol http
80fixup protocol h323 1720fixup protocol rsh 514fixup
protocol smtp 25fixup protocol sqlnet 1521fixup protocol
sip 5060fixup protocol skinny 2000names!--- Access
Control List (ACL) configured to bypass !--- Network
Address Translation (NAT) for the L2TP IP pool. access-
list nonat permit ip 20.1.1.0 255.255.255.0 50.1.1.0
255.255.255.0!--- ACL configured to permit L2TP traffic
(UDP port 1701). access-list l2tp permit udp host
171.68.9.57 any eq 1701no pagerlogging onlogging console
debugginglogging buffered debugginginterface ethernet0
10basetinterface ethernet1 10basetmtu outside 1500mtu
inside 1500ip address outside 171.68.9.57
255.255.255.0ip address inside 20.1.1.1 255.255.255.0ip
audit info action alarmip audit attack action alarm!---
Pool for L2TP address assignment. ip local pool l2tp
50.1.1.1-50.1.1.5pdm history enablearp timeout 14400!---
NAT configuration that matches previously defined !---
ACL for the L2TP IP pool.nat (inside) 0 access-list
nonatroute outside 0.0.0.0 0.0.0.0 171.68.9.1 1timeout
xlate 3:00:00timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 rpc 0:10:00 h3230:05:00 sip 0:30:00
sip_media 0:02:00timeout uauth 0:05:00 absoluteaaa-
server TACACS+ protocol tacacs+aaa-server RADIUS
protocol radius!--- AAA (RADIUS) server
configuration.aaa-server RADIUS (inside) host 20.1.1.2
cisco timeout 5no snmp-server locationno snmp-server
contactsnmp-server community publicno snmp-server enable
trapsfloodguard enable!--- sysopt command entry to
permit L2TP !--- traffic, while bypassing all
ACLs.sysopt connection permit-l2tpno sysopt route dnat!-
-- The IPsec configuration.crypto ipsec transform-set
l2tp esp-des esp-md5-hmac!--- Only transport mode is
supported.crypto ipsec transform-set l2tp mode
transportcrypto ipsec security-association lifetime
seconds 3600crypto dynamic-map dyna 20 match address
l2tpcrypto dynamic-map dyna 20 set transform-set
l2tpcrypto map mymap 10 ipsec-isakmp dynamic dynacrypto
map mymap client authentication RADIUScrypto map mymap
interface outside!--- The IKE configuration.isakmp
enable outsideisakmp policy 20 authentication rsa-
sigisakmp policy 20 encryption desisakmp policy 20 hash
md5isakmp policy 20 group 1isakmp policy 20 lifetime
86400ca identity sjvpn
171.68.9.149:/certsrv/mscep/mscep.dllca configure sjvpn
ra 1 20 crloptionaltelnet 171.68.9.0 255.255.255.0
```

```
insidetelnet 20.1.1.2 255.255.255.255 insidetelnet
timeout 60ssh timeout 5!--- The L2TP configuration
parameters.vpdn group l2tpipsec accept dialin l2tpvpdn
group l2tpipsec ppp authentication chapvpdn group
l2tpipsec ppp authentication mschapvpdn group l2tpipsec
client configuration address local l2tpvpdn group
l2tpipsec client configuration dns 20.1.1.250
20.1.1.251vpdn group l2tpipsec client configuration wins
20.1.1.250vpdn group l2tpipsec client authentication aaa
RADIUSvpdn group l2tpipsec client accounting RADIUSvpdn
group l2tpipsec l2tp tunnel hello 60vpdn enable
outsideterminal width
80Cryptochecksum:06a53009d1e9f04740256d9f0fb82837:
end[OK]
```

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.**

- **show crypto ca cert**? Отображает информацию о вашем сертификате, сертификате CA и любых сертификатах Центра регистрации (RA).`Certificate Status: Available Certificate Serial Number: 03716308000000000022 Key Usage: General Purpose Subject Name Name: PIX-506-2.sjvpn.com Validity Date: start date: 16:29:10 Apr 27 2001 end date: 16:39:10 Apr 27 2002 RA Signature Certificate Status: Available Certificate Serial Number: 0347dc82000000000002 Key Usage: Signature CN = scott OU = tac O = cisco L = san jose ST = ca C = US EA =<16> zaahmed@cisco.com Validity Date: start date: 18:47:45 Jul 27 2000 end date: 18:57:45 Jul 27 2001 CA Certificate Status: Available Certificate Serial Number: 1102485095cbf8b3415b2e96e86800d1 Key Usage: Signature CN = zakca OU = vpn O = cisco L = sj ST = california C = US EA =<16> zaahmed@cisco.com Validity Date: start date: 03:15:09 Jul 27 2000 end date: 03:23:48 Jul 27 2002 RA KeyEncipher Certificate Status: Available Certificate Serial Number: 0347df0d000000000003 Key Usage: Encryption CN = scott OU = tac O = cisco L = san jose ST = ca C = US EA =<16> zaahmed@cisco.com Validity Date: start date: 18:47:46 Jul 27 2000 end date: 18:57:46 Jul 27 2001`
- **show crypto isakmp sa — отображает все текущие IKE SA на одноранговом узле.**`dst src state pending created 171.68.9.57 171.68.9.149 QM_IDLE 0 1`
- **show crypto ipsec sa — отображает настройки, используемые текущими SA.**`interface: outside Crypto map tag: mymap, local addr. 171.68.9.57 local ident (addr/mask/prot/port): (171.68.9.57/255.255.255.255/17/1701) remote ident (addr/mask/prot/port): (171.68.9.149/255.255.255.255/17/1701) current_peer: 171.68.9.149 dynamic allocated peer ip: 0.0.0.0 PERMIT, flags={reassembly_needed,transport_parent,} #pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20 #pkts decaps: 45, #pkts decrypt: 45, #pkts verify 45 #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.: 171.68.9.57, remote crypto endpt.: 171.68.9.149 path mtu 1500, ipsec overhead 36, media mtu 1500 current outbound spi: a8c54ec8 inbound esp sas: spi: 0xfbc9db43(4224310083) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 1, crypto map: mymap sa timing: remaining key lifetime (k/sec): (99994/807) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xa8c54ec8(2831503048) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 2, crypto map: mymap sa timing: remaining key lifetime (k/sec): (99999/807) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:`
- **show vpdn tunnel**? Отображает информацию об активном L2TP или туннелях Level 2 Forwarding (L2F) в виртуальной частной коммутируемой сети (VPDN).`L2TP Tunnel Information (Total tunnels=1 sessions=1) Tunnel id 4 is up, remote id is 19, 1 active sessions Tunnel state is established, time since change 96 secs Remote Internet Address`

```
171.68.9.149, port 1701 Local Internet Address 171.68.9.57, port 1701 15 packets sent, 38
received, 420 bytes sent, 3758 received Control Ns 3, Nr 5 Local RWS 16, Remote RWS 8
Retransmission time 1, max 1 seconds Unsent queuesize 0, max 0 Resend queuesize 0, max 1
Total resends 0, ZLB ACKs 3 Retransmit time distribution: 0 0 0 0 0 0 0 0 % No active PPTP
tunnels PIX-506-2# sh uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 2
vpdn user 'vpnclient' at 50.1.1.1, authenticated
```

- **show vpdn session**? Отображает информацию об активном L2TP или сеансах L2F в VPDN.
```
L2TP Session Information (Total tunnels=1 sessions=1) Call id 4 is up on tunnel id 4
Remote tunnel name is zaahmed-pc Internet Address is 171.68.9.149 Session username is
vpnclient, state is established Time since change 201 secs, interface outside Remote call id
is 1 PPP interface id is 1 15 packets sent, 56 received, 420 bytes sent, 5702 received
Sequencing is off
```
- **show vpdn pppinterface**? Отображает статус и статистику виртуального интерфейса PPP, который был создан для туннеля PPTP для интерфейсного значения идентификации от **команды show vpdn session**.
```
PPP virtual interface id = 1 PPP authentication protocol is
CHAP Client ip address is 50.1.1.1 Transmitted Pkts: 15, Received Pkts: 56, Error Pkts: 0
MPPE key strength is None MPPE_Encrypt_Pkts: 0, MPPE_Encrypt_Bytes: 0 MPPE_Decrypt_Pkts: 0,
MPPE_Decrypt_Bytes: 0 Rcvd_Out_Of_Seq_MPPE_Pkts: 0
```
- **покажите uauth**? Отображает информацию о проверке подлинности и авторизация текущего пользователя.
```
Current Most Seen Authenticated Users 1 2 Authen In Progress 0 2
vpdn user 'vpnclient' at 50.1.1.1, authenticated
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **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– показывает события IPSec.**
- **debug crypto isakmp – отображает сообщения о событиях IKE.**
- **debug crypto engine?** Отображает сообщения отладки о ядрах шифрования, которые выполняют шифрование и расшифровку.
- **debug ppp io - вывод сведений о пакетах для виртуального интерфейса PPTP PPP.**
- **debug crypto ca**? Отображает сообщения отладки, которыми обмениваются с CA.
- **debug ppp error – отображает ошибки протокола и статистику ошибок, связанных с согласованием и функционированием PPP-соединения.**
- **debug vpdn error– показывает ошибки, не позволяющие установить туннель или вызывающие закрытие установленного туннеля.**
- **debug vpdn packet – отображает ошибки и события L2TP, которые сопровождают нормальную установку туннеля или завершение VPDN.**
- **debug vpdn event?** Отображает сообщения о событиях, которые являются частью обычной установки туннеля PPP или завершения.
- **debug ppp uauth - показывает сообщения отладки аутентификации пользователей AAA виртуального интерфейса PPTP PPP.**

Пример результата отладки

Это - выборка хорошей отладки на Межсетевом экране PIX.

```
crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57 ISAKMP: Created a peer node for
171.68.9.149 OAK_MM exchange ISAKMP (0): processing SA payload. message ID = 0 ISAKMP (0):
Checking ISAKMP transform 1 against priority 20 policy ISAKMP: encryption DES-CBC ISAKMP: hash
MD5 ISAKMP: default group 1 ISAKMP: auth RSA sig ISAKMP: life type in seconds ISAKMP: life
duration (VPI) of 0x0 0x0 0xe 0x10 ISAKMP (0): atts are acceptable. Next payload is 0 ISAKMP
(0): processing vendor id payload ISAKMP (0): speaking to a MSWIN2K client ISAKMP (0): SA is
doing RSA signature authentication using id type ID_FQDN return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57 OAK_MM exchange ISAKMP (0):
processing KE payload. message ID = 0 ISAKMP (0): processing NONCE payload. message ID = 0
return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57
OAK_MM exchange ISAKMP (0): processing ID payload. message ID = 0 ISAKMP (0): processing CERT
payload. message ID = 0 ISAKMP (0): processing a CT_X509_SIGNATURE cert CRYPTO_PKI: status = 0:
crl check ignored PKI: key process suspended and continued CRYPTO_PKI: WARNING: Certificate,
private key or CRL was not found while selecting CRL CRYPTO_PKI: cert revocation status unknown.
ISAKMP (0): cert approved with warning ISAKMP (0): processing SIG payload. message ID = 0 ISAKMP
(0): processing CERT_REQ payload. message ID = 0 ISAKMP (0): peer wants a CT_X509_SIGNATURE cert
ISAKMP (0): SA has been authenticated ISAKMP (0): ID payload next-payload : 6 type : 2 protocol
: 17 port : 500 length : 23 ISAKMP (0): Total payload length: 27 return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57 OAK_QM exchange
oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID =
3800855889 ISAKMP : Checking IPSec proposal 1 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in
transform: ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x0 0x3 0x84
ISAKMP: SA life type in kilobytes ISAKMP: SA life duration (VPI) of 0x0 0x1 0x86 0xa0 ISAKMP:
encaps is 2 ISAKMP: authenticator is HMAC-MD5 ISAKMP (0): atts are
acceptable.IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest=
171.68.9.57, src= 171.68.9.149, dest_proxy= 171.68.9.57/255.255.255.255/17/1701 (type=1),
src_proxy= 171.68.9.149/255.255.255.255/17/1701 (type=1), protocol= ESP, transform= esp-des esp-
md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0 ISAKMP (0):
processing NONCE payload. message ID = 3800855889 ISAKMP (0): processing ID payload. message ID
= 3800855889 ISAKMP (0): ID_IPV4_ADDR src 171.68.9.149 prot 17 port 1701 ISAKMP (0): processing
ID payload. message ID = 3800855889 ISAKMP (0): ID_IPV4_ADDR dst 171.68.9.57 prot 17 port
1701IPSEC(key_engine): got a queue event... IPSEC(spi_response): getting spi
0xfbc9db43(4224310083) for SA from 171.68.9.149 to 171.68.9.57 for prot 3 return status is
IKMP_NO_ERROR crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57 OAK_QM exchange
oakley_process_quick_mode: OAK_QM_AUTH_AWAIT ISAKMP (0): Creating IPSec SAs inbound SA from
171.68.9.149 to 171.68.9.57 (proxy 171.68.9.149 to 171.68.9.57) has spi 4224310083 and conn_id 1
and flags 0 lifetime of 900 seconds lifetime of 100000 kilobytes outbound SA from 171.68.9.57 to
171.68.9.149 (proxy 171.68.9.57 to 171.68.9.149) has spi 2831503048 and conn_id 2 and flags 0
lifetime of 900 seconds lifetime of 100000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): , (key eng. msg.) dest= 171.68.9.57, src= 171.68.9.149, dest_proxy=
171.68.9.57/0.0.0.0/17/1701 (type=1), src_proxy= 171.68.9.149/0.0.0.0/17/1701 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 900s and 100000kb, spi=
0xfbc9db43(4224310083), conn_id= 1, keysize= 0, flags= 0x0 IPSEC(initialize_sas): , (key eng.
msg.) src= 171.68.9.57, dest= 171.68.9.149, src_proxy= 171.68.9.57/0.0.0.0/17/1701 (type=1),
dest_proxy= 171.68.9.149/0.0.0.0/17/1701 (type=1), protocol= ESP, transform= esp-des esp-md5-
hmac , lifedur= 900s and 100000kb, spi= 0xa8c54ec8(2831503048), conn_id= 2, keysize= 0, flags=
0x0 return status is IKMP_NO_ERROR show log 603102: PPP virtual interface 1 - user: vpnclient
aaa authentication started 603103: PPP virtual interface 1 - user: vpnclient aaa authentication
succeed 109011: Authen Session Start: user 'vpnclient', sid 0 603106: L2TP Tunnel created,
tunnel_id is 1, remote_peer_ip is 171.68.9.149 ppp_virtual_interface_id is 1, client_dynamic_ip
is 50.1.1.1 username is vpnclient
```

Отладка, подходящая для регистрации в CA

```
CI thread sleeps! Crypto CA thread wakes up!% % Start certificate enrollment .. % The subject
name in the certificate will be: PIX-506-2.sjvpn.com   CI thread wakes up!% Certificate request
sent to Certificate Authority % The certificate request fingerprint will be displayed. PIX-506-
2(config)# PIX-506-2(config)#     Fingerprint:  d8475977 7198ef1f 17086f56 9e3f7a89 CRYPTO_PKI:
```

```
transaction PKCSReq completed CRYPTO_PKI: status: Crypto CA thread sleeps! PKI: key process
suspended and continued CRYPTO_PKI: http connection opened CRYPTO_PKI:  received msg of 711
bytes CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found while selecting CRL
CRYPTO_PKI: signed attr: pki-message-type: 13 01 33 CRYPTO_PKI: signed attr: pki-status: 13 01
33 CRYPTO_PKI: signed attr: pki-recipient-nonce: 04 10 70 0d 4e e8 03 09 71 4e c8 24 7a 2b 03 70
55 97 CRYPTO_PKI: signed attr: pki-transaction-id: 13 20 65 66 31 32 32 31 30 33 31 37 30 61 30
38 65 32 33 38 38 35 61 36 30 65 32 35 31 31 34 66 62 37 CRYPTO_PKI: status = 102: certificate
request pending CRYPTO_PKI: http connection opened CRYPTO_PKI:  received msg of 711 bytes
CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found while selecting CRL
CRYPTO_PKI: signed attr: pki-message-type: 13 01 33 CRYPTO_PKI: signed attr: pki-status: 13 01
33 CRYPTO_PKI: signed attr: pki-recipient-nonce: 04 10 c8 9f 97 4d 88 24 92 a5 3b ba 9e bc d6 7c
75 57 CRYPTO_PKI: signed attr: pki-transaction-id: 13 20 65 66 31 32 32 31 30 33 31 37 30 61 30
38 65 32 33 38 38 35 61 36 30 65 32 35 31 31 34 66 62 37 CRYPTO_PKI: status = 102: certificate
request pending !--- After approval from CA. Crypto CA thread wakes up! CRYPTO_PKI: resend
GetCertInitial, 1 Crypto CA thread sleeps! CRYPTO_PKI: resend GetCertInitial for session: 0
CRYPTO_PKI: http connection opened The certificate has been granted by CA! CRYPTO_PKI: received
msg of 1990 bytes CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found while
selecting CRL PKI: key process suspended and continued CRYPTO_PKI: signed attr: pki-message-
type: 13 01 33 CRYPTO_PKI: signed attr: pki-status: 13 01 30 CRYPTO_PKI: signed attr: pki-
recipient-nonce: 04 10 c8 9f 97 4d 88 24 92 a5 3b ba 9e bc d6 7c 75 57 CRYPTO_PKI: signed attr:
pki-transaction-id: 13 20 65 66 31 32 32 31 30 33 31 37 30 61 30 38 65 32 33 38 38 35 61 36 30
65 32 35 31 31 34 66 62 37 CRYPTO_PKI: status = 100: certificate is granted CRYPTO_PKI: WARNING:
Certificate, private key or CRL was not found while selecting CRL CRYPTO_PKI: All enrollment
requests completed. CRYPTO_PKI: All enrollment requests completed. CRYPTO_PKI: WARNING:
Certificate, private key or CRL was not found while selecting CRL
```

Отладка, не подходящая для регистрации в CA

В данном примере неправильный синтаксис URL использовался в команде **ca identity**:

```
CI thread sleeps! Crypto CA thread wakes up! CRYPTO_PKI: http connection opened
msgsym(GETCARACERT, CRYPTO)! %Error in connection to Certificate Authority: status = FAIL
CRYPTO_PKI: status = 266: failed to verify CRYPTO_PKI: transaction GetCACert completed Crypto CA
thread sleeps!
```

Если режим регистрации был задан так же CA вместо как RA, то вы получаете эту отладку:

```
CI thread sleeps! Crypto CA thread wakes up! CRYPTO_PKI: http connection opened Certificate has
the following attributes: Fingerprint: 49dc7b2a cd5fc573 6c774840 e58cf178 CRYPTO_PKI:
transaction GetCACert completed CRYPTO_PKI: Error:  Invalid format for BER encoding while
CRYPTO_PKI: can not set ca cert object. CRYPTO_PKI: status = 65535: failed to process RA
certiifcate Crypto CA thread sleeps!
```

В данном примере отсутствует **команда mode transport**:

```
ISAKMP:      SA life type in seconds ISAKMP:      SA life duration (VPI) of  0x0 0x0 0x70 0x80
ISAKMP:      SA life type in kilobytes ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      encaps is 2 ISAKMP:      authenticator is HMAC-MD5IPSEC(validate_proposal): invalid
transform proposal flags -- 0x0
```

В этих выходных данных отсутствует команда **crypto map mymap 10 ipsec-isakmp dynamic dyna**, и это сообщение может появиться в отладке:

```
no IPSEC cryptomap exists for local address a.b.c.d
```

Дополнительные сведения

- Страницы технической поддержки технологии RADIUS
- Справочник по командам PIX
- Страница поддержки PIX
- Страница технической поддержки протоколов согласования IPSec и IKE
- Запросы комментариев (RFC)

- Cisco Systems – техническая поддержка и документация