

# IPsec ASA и отладки IKE (агрессивный режим IKEv1) устраняющий неполадки Технические примечаний

## Содержание

[Введение](#)

[Базовая проблема](#)

[Сценарий](#)

[Используемые команды отладки](#)

[Конфигурация ASA](#)

[Отладка](#)

[Туннельная проверка](#)

[ISAKMP](#)

[IPSec](#)

[Дополнительные сведения](#)

## Введение

Когда и агрессивный режим и предварительный общий ключ (PSK) используются, этот документ описывает отладки на устройстве адаптивной защиты Cisco (ASA). Также обсуждается превращение определенных отладочных команд в конфигурацию. Cisco рекомендует иметь базовые знания о IPsec и Протоколе IKE.

Этот документ не обсуждает проходящий трафик после того, как был установлен туннель.

## Базовая проблема

IKE и отладки IPsec являются иногда загадочными, но можно использовать их для понимания проблем с установлением VPN-туннеля IPsec.

## Сценарий

Агрессивный режим, как правило, используется в случае Легкой VPN (EzVPN) с программным обеспечением (Cisco VPN Client) и аппаратные клиенты (Устройство адаптивной безопасности Cisco ASA 5505 или Cisco IOS<sup>?</sup> Программные маршрутизаторы), но только когда используется предварительный общий ключ. Отличный от главного режим, агрессивный режим состоит из трех сообщений.

Отладки от ASA, который работает под управлением ПО версии 8.3.2 и действует как сервер EzVPN. Клиент EzVPN является клиентским программным обеспечением.

## Используемые команды отладки

Это команды отладки, используемые в этом документе:

```
debug crypto isakmp 127
debug crypto ipsec 127
```

## Конфигурация ASA

Конфигурация ASA в данном примере предназначена, чтобы быть строго основной; никакие внешние серверы не используются.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.48.67.14 255.255.254.0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac

crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

crypto dynamic-map DYN 10 set transform-set TRA
crypto dynamic-map DYN 10 set reverse-route

crypto map MAP 65000 ipsec-isakmp dynamic DYN
crypto map MAP interface outside
crypto isakmp enable outside

crypto isakmp policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400

username cisco password cisco
username cisco attributes
vpn-framed-ip-address 192.168.1.100 255.255.255.0

tunnel-group EZ type remote-access
tunnel-group EZ general-attributes
 default-group-policy EZ
tunnel-group EZ ipsec-attributes
 pre-shared-key *****

group-policy EZ internal
group-policy EZ attributes
 password-storage enable
 dns-server value 192.168.1.99
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelall
 split-tunnel-network-list value split
 default-domain value jyoungta-labdomain.cisco.com
```

# Отладка

Примечание: [Прежде чем выполнять какие-либо команды отладки, ознакомьтесь с документом "Важные сведения о командах отладки".](#)

Описание сообщения сервера	Отладка		Описание сообщения клиента
	49711:28:30.28908/24/12Sev=Info/6IKE/0x6300003B Попытка установить соединение с 64.102.156.88. 49811:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_INITIALEvent: EV_INITIATOR 49911:28:30.29708/24/12Sev=Info/4IKE/0x63000001 Начинание переговоров 1-ой фазы протокола IKE 50011:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_GEN_DHKEY 50111:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_BLD_MSG 50211:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_START_RETRY_TMR 50311:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_SND_MSG		Агрессивный режим запускается. Создайте AM1. Этот процесс включает: - HDR ISAKMP - Устройство безопасности (SA), которое содержит всех, преобразовывает информационные наполнения и предложения, поддерживаемые клиентом - Информационное наполнение Обмена ключами - ID инициатора фазы 1 - Параметр
	50411:28:30.30408/24/12Sev=Info/4IKE/0x63000013 ПЕРЕДАВАЯ>>> AG ISAKMP OAK (SA, KE, NON, ID, VID (Xauth), VID (dpd), VID (Frag), VID (Nat-T), VID (Unity)) к 64.102.156.88		Передайте AM1.
	<===== Агрессивное сообщение 1 (AM1) =====		
Получите AM1 от клиента.	24 августа 11:31:03 [IKEv1] IP = 64.102.156.87, IKE_DECODE ПОЛУЧИЛ сообщение (msgid=0) с информационными наполнениями: HDR + SA (1) + KE (4) + ПАРАМЕТР (10) + ID (5) + ПОСТАВЩИК (13)	50611:28:30.33308/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_WAIT_MSG2Event: EV_NO_EVENT	Ждите ответа от сервера.

	+ ПОСТАВЩИК (13) + ПОСТАВЩИК (13) + ПОСТАВЩИК (13) + ПОСТАВЩИК (13) + NONE (0) общая длина: 849		
Процесс AM1. Сравните полученные предложения, и преобразовывает с уже настроенными для соответствий. Соответствующая конфигурация: ISAKMP включен на интерфейсе, и по крайней мере одна политика определена, что соответствия, что передал клиент: crypto isakmp enable outside crypto isakmp policy 10 authentication pre- share encryption aes hash sha group 2 lifetime 86400 Туннельная группа, совпадающая с идентичностью, называет подарок: tunnel-group EZ type remote-access tunnel-group EZ general-attributes default-group-policy EZ tunnel-group EZ ipsec- attributes pre-shared-key cisco	24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, обрабатывая информационное наполнение SA 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, обрабатывая ке информационное наполнение 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, обрабатывая информационное наполнение ISA_KE 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, обрабатывая информационное наполнение параметра 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, обрабатывая информационное наполнение ID 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, обрабатывая информационное наполнение VID 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, Полученный xauth V6 VID 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, обрабатывая информационное наполнение VID 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, полученный VID DPD 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, обрабатывая информационное наполнение VID 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, полученный VID фрагментации 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, Узел IKE включал флаги возможности фрагментации IKE: Основной Mode:TrueAggressive Mode:False 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, обрабатывая информационное наполнение VID 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, Полученная версия прохождения NAT 02 VID 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, обрабатывая информационное наполнение VID 24 августа 11:31:03 [IKEv1 DEBUG] IP = 64.102.156.87, Полученный VID клиента Cisco Unity 24 августа 11:31:03 [IKEv1] IP = 64.102.156.87, Соединение приземлилось на tunnel_group ipsec 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, обрабатывая информационное наполнение IKE SA 24 августа 11:31:03 [IKEv1] Фаза 1 failure:Mismatched типы атрибутов для Группы класса Description:Rcv'd: Группа 2Cfg'd: Группа 5 24 августа 11:31:03 [IKEv1] Фаза 1 failure:Mismatched типы атрибутов для Группы класса Description:Rcv'd: Группа 2Cfg'd: Группа 5		



<p>- аутентификация - Информационное наполнение обнаружения Технологии NAT</p>	<p>= 64.102.156.87, создавая информационное наполнение параметра 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, Генерируя ключи для Респондента... 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, создавая информационное наполнение ID 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, создавая информационное наполнение хэша 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, Вычисляя хэш для ISAKMP 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, создавая информационное наполнение VID Cisco Unity 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, создавая информационное наполнение xauth V6 VID 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, создавая dpd vid информационное наполнение 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, создавая версию VID прохождения NAT 02 информационных наполнения 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, создавая информационное наполнение Обнаружения NAT 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, вычислительный хэш Обнаружения NAT 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, создавая информационное наполнение Обнаружения NAT 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, вычислительный хэш Обнаружения NAT 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, создавая VID Фрагментации + расширило информационное наполнение возможностей 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, создавая информационное наполнение VID 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, Передает VID GW Vpn3000/Cisco ASA Altiga/Cisco</p>	
<p>Передайте AM2.</p>	<p>24 августа 11:31:03 [IKEv1] IP = 64.102.156.87, сообщение (msgid=0) ПЕРЕДАЧИ IKE_DECODE с информационными наполнениями: HDR + SA (1) + KE (4) + ПАРАМЕТР (10) + ID (5) + ХЭШ (8) + ПОСТАВЩИК (13) + ПОСТАВЩИК (13) + ПОСТАВЩИК (13) + ПОСТАВЩИК (13) + NAT-D (130) + NAT-D (130) + ПОСТАВЩИК (13) + ПОСТАВЩИК</p>	

	(13) + NONE (0) общая длина: 444	
	===== <b> Агрессивное сообщение 2 (AM2)</b> ===== =====>	
	50711:28:30.40208/24/12Sev=Info/5IKE/0x6300002F Полученный Пакет ISAKMP: взаимодействуйте = 64.102.156.8 50811:28:30.40308/24/12Sev=Info/4IKE/0x63000014 ПОЛУЧАЯ <<<AG ISAKMP OAK (SA, KE, NON, ID, XЭШ, VID (Unity), VID (Xauth), VID (dpd), VID (Nat-T), NAT-D, NAT-D, VID (Frag), VID (?)) от 64.102.156.88 51011:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_RCVD_MSG	Получите AM2.
	51111:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Узел является Cisco Unity совместимый узел 51211:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Узел поддерживает XAUTH 51311:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Узел поддерживает DPD 51411:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Узел поддерживает NAT-T 51511:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Узел поддерживает информационные наполнения фрагментации IKE 51611:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_GEN_SKEYID 51711:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_AUTHENTICATE_PEER 51811:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_ADJUST_PORT 51911:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_CRYPTO_ACTIVE	AM 2 процесса.
	52011:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Event: EV_BLD_MSG] 52111:28:30.42208/24/12Sev=Debug/8IKE/0x63000001 Идентификатор поставщика IOS Contruction запустился 52211:28:30.42208/24/12Sev=Info/6IKE/0x63000001 Идентификатор поставщика IOS успешный Contruction	Создайте AM3. Этот процесс включает Клиентскую Аутентификацию. На этом этапе все данные, важные для шифрования, были уже переданы.
	52311:28:30.42308/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:I_Cookie=D56197780D7BE3E5	Передайте AM3.

	R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Event: EV_SND_MSG 52411:28:30.42308/24/12Sev=Info/4IKE/0x63000013 ПЕРЕДАВАЯ>>> AG ISAKMP OAK * (ХЭШ, NOTIFY:STATUS_INITIAL_CONTACT, NAT-D, NAT-D, VID (?), VID (Unity)) к 64.102.156.88	
	<===== Агрессивное сообщение 3 (AM3) =====	
Получите AM3 от клиента.	24 августа 11:31:03 [IKEv1] IP = 64.102.156.87, IKE_DECODE ПОЛУЧИЛ сообщение (msgid=0) с информационными наполнениями: HDR + ХЭШ (8) + УВЕДОМЛЯЕТ (11) + NAT-D (130) + NAT-D (130) + ПОСТАВЩИК (13) + ПОСТАВЩИК (13) + NONE (0) общая длина: 168	
AM 3 процесса. Подтвердите обход NAT (NAT-T) использование. Обе стороны теперь готовы запустить шифрование трафика.	24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, обрабатывая информационное наполнение хэша 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, Вычисляя хэш для ISAKMP 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, обработка уведомляет информационное наполнение 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, обрабатывая информационное наполнение Обнаружения NAT 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, вычислительный хэш Обнаружения NAT 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, обрабатывая информационное наполнение Обнаружения NAT 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, вычислительный хэш Обнаружения NAT 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, обрабатывая информационное наполнение VID 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, Обработывая информационное наполнение Идентификатора поставщика IOS/PIX (версия: 1.0.0, возможности: 00000408) 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, обрабатывая информационное наполнение VID 24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, Полученный VID клиента Cisco Unity 24 августа 11:31:03 [IKEv1] Группа = ipsec, IP = 64.102.156.87, Автоматическое Обнаружение NAT Статус: Удаленный endISbehind NAT deviceThisend HE находится позади устройства NAT	
Иницируйте Фазу 1.5 (XAUTH) и запросите учетные	24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, создавая пробел хеширует информационное наполнение	



данные пользователя.	24 августа 11:31:03 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, создавая qm хеширует информационное наполнение 24 августа 11:31:03 [IKEv1] IP = 64.102.156.87, сообщение (msgid=fb709d4d) ПЕРЕДАЧИ IKE_DECODE с информационными наполнениями: HDR + ХЭШ (8) + ATTR (14) + NONE (0) общая длина: 72	
	===== Xauth - Запрос Учетных данных =====>	
	53511:28:30.43008/24/12Sev=Info/4IKE/0x63000014 ПОЛУЧАЯ <<<ISAKMP OAK TRANS * (ХЭШ, ATTR) от 64.102.156.88 53611:28:30.43108/24/12Sev=Decode/11IKE/0x63000001 Заголовок ISAKMP Инициатор COOKIE:D56197780D7BE3E5 Респондент COOKIE:1B301D2DE710EDA0 Следующий Payload:Hash Ver (Hex):10 Exchange Type:Transaction Flags:(Encryption) MessageID (Hex): FB709D4D Длина: 76 Хэш информационного наполнения Следующее информационное наполнение: атрибуты Зарезервированный: 00 Длина полезных данных: 24 Данные (в Hex): C779D5CVC5C75E3576C478A15A7CAB8A83A232D0 Атрибуты информационного наполнения Следующее информационное наполнение: Нет Зарезервированный: 00 Длина полезных данных: 20 Введите : ISAKMP_CFG_REQUEST Зарезервированный: 00 Идентификатор: 0000 Тип XAUTH: общего назначения Имя пользователя XAUTH: (пустой) Пароль пользователя XAUTH: (пустой) 53711:28:30.43108/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> TM:MsgID=FB709D4DCurState: TM_INITIALEvent: EV_RCVD_MSG	Получите Запрос на аутентификацию. Дешифрованное информационное наполнение показывает пустые поля имени пользователя и пароля.
	53811:28:30.43108/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent: EV_INIT_XAUTH 53911:28:30.43108/24/12 Sev=Debug/7IKE/0x63000076 Трассировка NAV-> TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent: EV_START_RETRY_TMR 54011:28:30.43208/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_NO_EVENT 541 11:28:36.41508/24/12Sev=Debug/7IKE/0x63000076	Иницируйте Фазу 1.5 (XAUTH). Иницируйте таймер повторной попытки, поскольку он ждет ввода пользователя. Когда таймер повторной

	Трассировка NAV-> TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_RCVD_USER_INPUT	попытки заканчивается, соединение автоматически разъединено.
	54211:28:36.41508/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_SND_MSG 54311:28:36.41508/24/12Sev=Info/4IKE/0x63000013 ПЕРЕДАВАЯ>>> ISAKMP OAK TRANS * (XЭШ, ATTR) к 64.102.156.88 54411:28:36.41508/24/12Sev=Decode/11IKE/0x63000001 Заголовок ISAKMP Инициатор COOKIE:D56197780D7BE3E5 Респондент COOKIE:1B301D2DE710EDA0 Следующий Payload:Hash Ver (Hex):10 Exchange Type:Transaction Flags:(Encryption) MessageID (Hex): FB709D4D Длина: 85 Хэш информационного наполнения Следующее информационное наполнение: атрибуты Зарезервированный: 00 Длина полезных данных: 24 Данные (в Hex): 1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5 Атрибуты информационного наполнения Следующее информационное наполнение: Нет Зарезервированный: 00 Длина полезных данных: 33 Введите : ISAKMP_CFG_REPLY Зарезервированный: 00 Идентификатор: 0000 Тип XAUTH: общего назначения Имя пользователя XAUTH: (данные, не отображенные) Пароль пользователя XAUTH: (данные, не отображенные)	Как только ввод пользователя получен, передайте учетные данные пользователя к серверу. Дешифрованное информационное наполнение показывает заполненный (но скрытый) поля имени пользователя и пароля. Отправьте запрос настройки режима (различные атрибуты).
	<b>&lt;===== Xauth - учетные данные пользователя =====&gt;</b>	
Получите учетные данные пользователя.	24 августа 11:31:09 [IKEv1] IP = 64.102.156.87, IKE_DECODE ПОЛУЧИЛ сообщение (msgid=fb709d4d) с информационными наполнениями: HDR + XЭШ (8) + ATTR (14) + NONE (0) общая длина: 85 24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, process_attr (): Введите!	
Учетные данные пользователя процесса. Проверьте учетные	24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, IP = 64.102.156.87, Обработывая атрибуты Ответа MODE_CFG. 24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec,	

<p>данные и генерируйте информационное наполнение настройки режима. Соответствующая конфигурация: username cisco password cisco</p>	<p>Имя пользователя = user1, IP = 64.102.156.87, IKEGetUserAttributes: основной DNS = 192.168.1.99 24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, IKEGetUserAttributes: вторичный DNS = очистился 24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, IKEGetUserAttributes: основной WINS = очистился 24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, IKEGetUserAttributes: вторичный WINS = очистился 24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, IKEGetUserAttributes: список разделенного туннелирования = разделение 24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, IKEGetUserAttributes: домен по умолчанию = jyoungta-labdomain. cisco . com 24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, IKEGetUserAttributes: Сжатие IP = отключенный 24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, IKEGetUserAttributes: Политика Разделенного туннелирования = Отключенный 24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, IKEGetUserAttributes: Параметр прокси Браузера = нет - модифицирует 24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, IKEGetUserAttributes: Обход Прокси Браузера, Локальный =, отключает 24 августа 11:31:09 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Пользователь (user1) аутентифицировалось.</p>	
<p>Передайте результат xauth.</p>	<p>24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, создавая пробел хеширует информационное наполнение 24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, создавая qm хеширует информационное наполнение 24 августа 11:31:09 [IKEv1] IP = 64.102.156.87, сообщение (msgid=5b6910ff) ПЕРЕДАЧИ IKE_DECODE с информационными наполнениями: HDR + ХЭШ (8) + ATTR (14) + NONE (0) общая длина: 64</p>	
	<p>=====<b>Xauth - Результат Авторизации</b>===== =====&gt;</p>	
	<p>54511:28:36.41608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-&gt; TM:MsgID=FB709D4DCurState:</p>	<p>Получите подлинные</p>

	<p>TM_XAUTHREQ_DONEEvent: EV_XAUTHREQ_DONE  54611:28:36.41608/24/12Sev=Debug/7IKE/0x63000076  Трассировка NAV-&gt; TM:MsgID=FB709D4DCurState:  TM_XAUTHREQ_DONEEvent: EV_NO_EVENT  54711:28:36.42408/24/12Sev=Info/5IKE/0x6300002F  Полученный Пакет ISAKMP: взаимодействуйте =  64.102.156.88  54811:28:36.42408/24/12Sev=Info/4IKE/0x63000014  ПОЛУЧАЯ &lt;&lt;&lt;ISAKMP OAK TRANS * (XЭШ, ATTR) от  64.102.156.88  54911:28:36.42508/24/12Sev=Decode/11IKE/0x6300000  1  Заголовок ISAKMP  Инициатор COOKIE:D56197780D7BE3E5  Респондент COOKIE:1B301D2DE710EDA0  Следующий Payload:Hash  Ver (Hex):10  Exchange Type:Transaction  Flags:(Encryption)  MessageID (Hex):5B6910FF  Длина: 76  Хэш информационного наполнения  Следующее информационное наполнение: атрибуты  Зарезервированный: 00  Длина полезных данных: 24  Данные (в Hex):  7DCF47827164198731639BFB7595F694C9DDFE85  Атрибуты информационного наполнения  Следующее информационное наполнение: Нет  Зарезервированный: 00  Длина полезных данных: 12  Введите : ISAKMP_CFG_SET  Зарезервированный: 00  Идентификатор: 0000  Статус XAUTH: проход  55011:28:36.42508/24/12Sev=Debug/7IKE/0x63000076  Трассировка NAV-&gt; TM:MsgID=5B6910FFCurState:  TM_INITIALEvent: EV_RCVD_MSG  55111:28:36.42508/24/12Sev=Debug/7IKE/0x63000076  Трассировка NAV-&gt; TM:MsgID=5B6910FFCurState:  TM_PCS_XAUTH_SETEvent: EV_INIT_XAUTH  55211:28:36.42508/24/12Sev=Debug/7IKE/0x63000076  Трассировка NAV-&gt; TM:MsgID=5B6910FFCurState:  TM_PCS_XAUTH_SETEvent: EV_CHK_AUTH_RESULT</p>	результаты и результаты процесса.
	55311:28:36.42508/24/12Sev=Info/4IKE/0x63000013 ПЕРЕДАВАЯ>>> ISAKMP OAK TRANS * (XЭШ, ATTR) к 64.102.156.88	Результат ACK.
	<===== Xauth - подтверждение =====	
Получите и обработайте ACK; никакой ответ от сервера.	24 августа 11:31:09 [IKEv1] IP = 64.102.156.87, IKE_DECODE ПОЛУЧИЛ сообщение (msgid=5b6910ff) с информационными наполнениями: HDR + XЭШ (8) + ATTR (14) + NONE (0) общая длина: 60	

	<p>24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, process_attr (): Введите!</p> <p>24 августа 11:31:09 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Обработывая атрибуты ACK cfg</p>	
	<p>55511:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-&gt; TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_XAUTH_DONE_SUC</p> <p>55611:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-&gt; TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_NO_EVENT</p> <p>55711:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-&gt; TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_TERM_REQUEST</p> <p>55811:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-&gt; TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_REMOVE</p> <p>55911:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-&gt; TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_NO_EVENT</p> <p>56011:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-&gt; SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_XAUTH_PROGEvent: EV_XAUTH_DONE_SUC</p> <p>56111:28:38.40608/24/12Sev=Debug/8IKE/0x6300004C Стартовый таймер DPD для IKE SA (I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0), sa-&gt; сообщают = 1, sa-&gt; dpd.worry_freq (mSec) = 5000</p> <p>56211:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-&gt; SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_MODECFG</p> <p>56311:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-&gt; SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_NO_EVENT</p> <p>56411:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-&gt; TM:MsgID=84B4B653CurState: TM_INITIAEvent: EV_INIT_MODECFG</p> <p>56511:28:38.40808/24/12Sev=Info/5IKE/0x6300005E Клиент, отправляющий запрос межсетевого экрана к концентратору</p> <p>56611:28:38.40908/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-&gt; TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_START_RETRY_TMR</p>	<p>Генерируйте запрос настройки режима. Дешифрованное информационное наполнение показывает запрошенные параметры от сервера.</p>
	<p>56711:28:38.40908/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-&gt; TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_SND_MSG</p> <p>56811:28:38.40908/24/12Sev=Info/4IKE/0x63000013</p>	<p>Отправьте запрос настройки режима.</p>

ПЕРЕДАВАЯ>>> ISAKMP OAK TRANS \* (ХЭШ, ATTR)  
к 64.102.156.88  
56911:28:38.62708/24/12Sev=Decode/11IKE/0x6300000  
1  
Заголовок ISAKMP  
Инициатор COOKIE:D56197780D7BE3E5  
Респондент COOKIE:1B301D2DE710EDA0  
Следующий Payload:Hash  
Ver (Hex):10  
Exchange Type:Transaction  
Flags:(Encryption)  
MessageID (Hex):84B4B653  
Длина: 183

Хэш информационного наполнения  
Следующее информационное наполнение: атрибуты  
Зарезервированный: 00  
Длина полезных данных: 24  
Данные (в Hex):  
81BFBF6721A744A815D69A315EF4AAA571D6B687

Атрибуты информационного наполнения  
Следующее информационное наполнение: Нет  
Зарезервированный: 00  
Длина полезных данных: 131  
Введите : ISAKMP\_CFG\_REQUEST  
Зарезервированный: 00  
Идентификатор: 0000  
Адрес IPv4: (пустой)  
Маска подсети IPv4: (пустой)  
DNS IPv4: (пустой)  
NBNS IPv4 (WINS): (пустой)  
Истечение адреса: (пустой)  
Расширение Cisco: Баннер: (пустой)  
Расширение Cisco: Сохраните PWD: (пустой)  
Расширение Cisco: Название Домена по умолчанию:  
(пустой)  
Расширение Cisco: Разделение Включает: (пустой)  
Расширение Cisco: Название Разделения DNS:  
(пустой)  
Расширение Cisco: Сделайте безопасную пересылку  
(PFS): (пустой)  
Неизвестный: (пустой)  
Расширение Cisco: Серверы резервного копирования:  
(пустой)  
Расширение Cisco: Разъединение Удаления Смарт-  
карты: (пустой)  
Версия приложения: клиент VPN Cisco Systems  
5.0.07.0290:WinNT  
Расширение Cisco: Тип Межсетевого экрана: (пустой)  
Расширение Cisco: Имя хоста Динамических DN:  
ATBASU-LABBOX

<===== запрос настройки режима

	=====		
<p>Получите запрос настройки режима.</p>	<p>24 августа 11:31:11 [IKEv1] IP = 64.102.156.87, IKE_DECODE ПОЛУЧИЛ сообщение (msgid=84b4b653) с информационными наполнениями: HDR + ХЭШ (8) + ATTR (14) + NONE (0) общая длина: 183</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, process_attr (): Введите!</p>	<p>57011:28:38.62808/24/12Sev = Debug/7IKE/0x63000076 Трассировка NAV-&gt; TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_NO_EVENT</p>	<p>Ждите ответа сервера.</p>
<p>Запрос настройки режима процесса. Многие из этих значений обычно настраиваются в групповой политике. Однако, так как сервер в данном примере имеет очень простую конфигурацию, вы не видите их здесь.</p>	<p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Обработывая атрибуты Запроса cfg</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, MODE_CFG: Полученный запрос об Адресе IPv4!</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, MODE_CFG: Полученный запрос о маске сети IPv4!</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, MODE_CFG: Полученный запрос об адресе сервера DNS!</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, MODE_CFG: Полученный запрос об адресе сервера WINS!</p> <p>24 августа 11:31:11 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Полученный неподдерживаемый атрибут режима транзакции: 5</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, MODE_CFG: Полученный запрос о Баннере!</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, MODE_CFG: Полученный запрос о Сохраняет настройку PW!</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87,</p>		

	<p>MODE_CFG: Полученный запрос о Названии Домена по умолчанию!  24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87,  MODE_CFG: Полученный запрос о Списке разделенных туннелей!  24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87,  MODE_CFG: Полученный запрос о Разделении DNS!  24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87,  MODE_CFG: Полученный запрос о значении безопасной пересылки (PFS)!  24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87,  MODE_CFG: Полученный запрос о Параметре прокси Клиентского браузера!  24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87,  MODE_CFG: Полученный запрос о резервном списке однорангового узла IPsec!  24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87,  MODE_CFG: Полученный запрос о Клиентском Значении Разъединения Удаления смарт-карты!  24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87,  MODE_CFG: Полученный запрос о Версии приложения!  24 августа 11:31:11 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Тип клиентской части: Версия приложения WinNTClient: 5.0.07.0290  24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87,  MODE_CFG: Полученный запрос о FWTYPE!  24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87,  MODE_CFG: Полученный запрос об имени хоста DHCP для DDNS: ATBASU-LABBOX!</p>	
<p>Создайте ответ настройки режима со всеми значениями, которые настроены. Соответствующая конфигурация: Обратите внимание в этом случае, пользователю всегда назначают тот же IP.  username cisco</p>	<p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Полученный адрес IP (192.168.1.100) до инициирования Cfg Режим (Xauth включил),  24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Передача маски подсети (255.255.255.0) удаленному клиенту  24 августа 11:31:11 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Назначенный закрытый IP - адрес 192.168.1.100 удаленному пользователю  24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec,</p>	



<pre>attributes vpn-framed-ip- address 192.168.1.100 255.255.255.0 group-policy EZ internal group-policy EZ attributes password-storage enabledns-server value 192.168.1.129 vpn-tunnel-protocol ikev1 split-tunnel-policy tunnelall split-tunnel-network- list value split default- domain value jyoungta- labdomain.cisco.com</pre>	<p>Имя пользователя = user1, IP = 64.102.156.87, создавая пробел хеширует информационное наполнение</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, construct_cfg_set: домен по умолчанию = jyoungta- labdomain.cisco . com</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Передает Атрибуты Прокси Клиентского браузера!</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, набор Прокси Браузера к Нет - Модифицирует. Данные Прокси браузера НЕ будут включены в ответ cfg режима</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Передает Разъединение Удаления смарт-карты Cisco, включают!!</p> <p>24 августа 11:31:11 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, создавая qm хеширует информационное наполнение</p>	
<p>Передайте ответ настройки режима.</p>	<p>24 августа 11:31:11 [IKEv1] IP = 64.102.156.87, сообщение (msgid=84b4b653) ПЕРЕДАЧИ IKE_DECODE с информационными наполнениями: HDR + ХЭШ (8) + ATTR (14) + NONE (0) общая длина: 215</p>	
	<p style="text-align: center;">===== Ответ настройки режима =====&gt;</p>	
	<p>57111:28:38.63808/24/12Sev=Info/5IKE/0x6300002F Полученный Пакет ISAKMP: взаимодействуйте = 64.102.156.88</p> <p>57211:28:38.63808/24/12Sev=Info/4IKE/0x63000014 ПОЛУЧАЯ &lt;&lt;&lt;ISAKMP OAK TRANS * (ХЭШ, ATTR) от 64.102.156.88</p> <p>57311:28:38.63908/24/12Sev=Decode/11IKE/0x6300000 1</p> <p>Заголовок ISAKMP Инициатор COOKIE:D56197780D7BE3E5 Респондент COOKIE:1B301D2DE710EDA0 Следующий Payload:Hash Ver (Hex):10 Exchange Type:Transaction Flags:(Encryption) MessageID (Hex):84B4B653 Длина: 220 Хэш информационного наполнения Следующее информационное наполнение: атрибуты Зарезервированный: 00 Длина полезных данных: 24 Данные (в Hex): 6DE2E70ACF6B1858846BC62E590C00A66745D14D Атрибуты информационного наполнения</p>	<p>Получите значения параметра настройки режима от сервера.</p>

	<p>Следующее информационное наполнение: Нет  Зарезервированный: 00  Длина полезных данных: 163  Введите : ISAKMP_CFG_REPLY  Зарезервированный: 00  Идентификатор: 0000  Адрес IPv4: 192.168.1.100  Маска подсети IPv4: 255.255.255.0  DNS IPv4: 192.168.1.99  Расширение Cisco: Сохраните PWD: Нет  Расширение Cisco: Название Домена по умолчанию:  jyoungta-labdomain. cisco . com  Расширение Cisco: Сделайте безопасную пересылку  (PFS): Нет  Версия приложения: версия 8.4 (4) 1 Cisco Systems,  Inc ASA5505, созданная разработчиками в четверг 14  июня 12 11:20  Расширение Cisco: Разъединение Удаления Смарт-  карты: Да</p>		
<p>Фаза 1 завершает на сервере. Иницируйте процесс режима Quick Mode (QM).</p>	<p>24 августа 11:31:13 [IKEv1 ДЕКОДИРУЕТ] IP = 64.102.156.87, Респондент IKE стартовый QM: идентификатор сообщения = 0e83792e 24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, обработка Быстрого режима Задержки, Обмен/RM Свидетельства/Сд елки происходящий DSID 24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Предварительный ARP запрос послал 192.168.1.100</p>	<p>57411:28:38.63908/24/12Sev = Debug/7IKE/0x63000076 Трассировка NAV-&gt; TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_RCVD_MSG 57511:28:38.63908/24/12Sev = Info/5IKE/0x63000010 MODE_CFG_REPLY: атрибут = INTERNAL_IPV4_ADDRESS: оцените = 192.168.1.100 57611:28:38.63908/24/12Sev=Info/ 5IKE/0x63000010 MODE_CFG_REPLY: атрибут = INTERNAL_IPV4_NETMASK: оцените = 255.255.255.0 57711:28:38.63908/24/12Sev = Info/5IKE/0x63000010 MODE_CFG_REPLY: атрибут = INTERNAL_IPV4_DNS (1): оцените = 192.168.1.99 57811:28:38.63908/24/12Sev=Info/ 5IKE/0x6300000D MODE_CFG_REPLY: атрибут = MODECFG_UNITY_SAVEPWD: значение = 0x00000000 57911:28:38.63908/24/12Sev=Info/ 5IKE/0x6300000E MODE_CFG_REPLY: атрибут = MODECFG_UNITY_DEFDOMAIN: значение = jyoungta- labdomain. cisco . com 58011:28:38.63908/24/12Sev = Info/5IKE/0x6300000D</p>	<p>Параметры процесса, и настраивают себя соответственно.</p>

	<p>24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, обработка Быстрого режима Резюме, Обмен/RM Свидетельства/Сделки DSID завершено</p> <p>24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, ФАЗА 1 ЗАВЕРШЕНА</p>	<p>MODE_CFG_REPLY: Атрибут = MODECFG_UNITY_PFS: значение = 0x00000000</p> <p>58111:28:38.63908/24/12Sev=Info/5IKE/0x6300000E</p> <p>MODE_CFG_REPLY: атрибут = APPLICATION_VERSION, оцените = версия 8.4 (4) 1 Cisco Systems, Inc ASA5505, созданная разработчики в четверг 14 июня 12 11:20</p> <p>58211:28:38.63908/24/12Sev = Info/5IKE/0x6300000D</p> <p>MODE_CFG_REPLY: атрибут = MODECFG_UNITY_SMARTCARD_REMOVAL_DISCONNECT: значение = 0x00000001</p> <p>58311:28:38.63908/24/12Sev = Info/5IKE/0x6300000D</p> <p>MODE_CFG_REPLY: Атрибут = Полученный и использующий NAT-T номер порта, значение = 0x00001194</p> <p>58411:28:39.36708/24/12Sev = Debug/9IKE/0x63000093</p> <p>Значение для параметра ini EnableDNSRedirection равняется 1</p> <p>58511:28:39.36708/24/12Sev = Debug/7IKE/0x63000076</p> <p>Трассировка NAV-&gt;</p> <p>TM:MsgID=84B4B653CurState: TM_MODECFG_DONEEvent: EV_MODECFG_DONE_SUC</p>	
<p>Создайте и передайте DPD за клиентом.</p>	<p>24 августа 11:31:13 [IKEv1] IP = 64.102.156.87, Тип проверки активности для этого соединения: DPD</p> <p>24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Запуская P1 повторно вводит таймер: 82080 секунд.</p> <p>24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, передача уведомляет сообщение</p> <p>24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, создавая пробел хеширует информационное наполнение</p> <p>24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, создавая qm хеширует информационное наполнение</p> <p>24 августа 11:31:13 [IKEv1] IP = 64.102.156.87, сообщение (msgid=be8f7821) ПЕРЕДАЧИ IKE_DECODE с информационными наполнениями:</p>		

	HDR + ХЭШ (8) + УВЕДОМЛЯЕТ (11) + NONE (0) общая длина: 92	
	===== <b>Dead Peer Detection (DPD)</b> ===== =====>	
	58811:28:39.79508/24/12Sev=Debug/7IKE/0x63000015 intf_data&colon; lcl=0x0501A8C0, mask=0x00FFFFFF, bcast=0xFF01A8C0, bcast_vra=0xFF07070A 58911:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:l_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_P2 59011:28:39.79508/24/12Sev=Info/4IKE/0x63000056 Полученный ключевой запрос от Драйвера: Локальный IP = 192.168.1.100, IP GW = 64.102.156.88, Удаленный IP = 0.0.0.0 59111:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> SA:l_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_ACTIVEEvent: EV_NO_EVENT 59211:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> QM:MsgID=0E83792ECurState: QM_INITIALEvent: EV_INITIATOR 59311:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> QM:MsgID=0E83792ECurState: QM_BLD_MSG1Event: EV_CHK_PFS 59411:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> QM:MsgID=0E83792ECurState: QM_BLD_MSG1Event: EV_BLD_MSG 59511:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> QM:MsgID=0E83792ECurState: QM_SND_MSG1Event: EV_START_RETRY_TMR	Иницируйте QM, Фазу 2. Создайте QM1. Этот процесс включает: - Хэш - SA со всеми предложениями по Фазе 2, поддерживаемыми клиентом, типом туннеля и шифрованием - Параметр - Идентификатор клиента - Proxy Id
	59611:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 Трассировка NAV-> QM:MsgID=0E83792ECurState: QM_SND_MSG1Event: EV_SND_MSG 59711:28:39.79608/24/12Sev=Info/4IKE/0x63000013 ПЕРЕДАВАЯ>>> QM ISAKMP OAK * (ХЭШ, SA, NON, ID, ID) к 64.102.156.88	Передайте QM1.
	<===== <b>сообщение 1 (QM1) быстрого режима</b> =====>	
Получите QM1.	24 августа 11:31:13 [IKEv1] IP = 64.102.156.87, IKE_DECODE ПОЛУЧИЛ сообщение (msgid=e83792e) с информационными наполнениями: HDR + ХЭШ (8) + SA (1) + ПАРАМЕТР (10) + ID (5) + ID (5) + NONE (0) общая длина: 1026	
Процесс QM1. Соответствующая конфигурация: username cisco attributes vpn-framed-ip- address 192.168.1.100 255.255.255.0 group-policy EZ internal	24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, обрабатывая информационное наполнение хэша 24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, обрабатывая информационное наполнение SA 24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87,	

<pre>group-policy EZ attributes password-storage enabledns-server value 192.168.1.129 vpn-tunnel-protocol ikev1 split-tunnel-policy tunnelall split-tunnel-network- list value split default- domain value jyoungta- labdomain.cisco.com</pre>	<p>обрабатывая информационное наполнение параметра</p> <p>24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, обрабатывая информационное наполнение ID</p> <p>24 августа 11:31:13 [IKEv1 ДЕКОДИРУЕТ] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, полученный ID_IPV4_ADDR ID 192.168.1.100</p> <p>24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Полученные удаленные данные Прокси-сервера в ID Payload:Address 192.168.1.100, Протокол 0, порт 0</p> <p>24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, обрабатывая информационное наполнение ID</p> <p>24 августа 11:31:13 [IKEv1 ДЕКОДИРУЕТ] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, полученный ID_IPV4_ADDR_SUBNET ID - 0.0.0.0 - 0.0.0.0</p> <p>24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Полученные данные Подсети Прокси локального IP в ID Payload:Address 0.0.0.0, Маска 0.0.0.0, Протокол 0, порт 0</p> <p>24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, QM IsRekeyed старый sa, не найденный адресом</p> <p>24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, проверка Статической криптокарты, проверяя карту ==карта, seq = 10...</p> <p>24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Проверка Статической криптокарты обошла: неполный Элемент криптокарты!</p> <p>24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Выбирая только Инкапсулированный Туннель UDP andUDP-Encapsulated-Transport определенный прохождением NAT</p> <p>24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Выбирая только Инкапсулированный Туннель UDP andUDP-Encapsulated-Transport определенный прохождением NAT</p> <p>24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Удаленный узел IKE настроил для криптокарты: out-dyn-map</p> <p>24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, обрабатывая информационное наполнение КОНТЕКСТА БЕЗОПАСНОСТИ IPSEC</p>	
--	---	--

Создайте QM2.  
Соответствующая конфигурация:  
tunnel-group EZ  
type **remote-access** !  
(tunnel type ra = tunnel  
type remote-access)  
crypto ipsec  
transform-  
set TRA **esp-aes esp-sha-hmac**  
crypto ipsec  
security-  
association **lifetime seconds 28800**  
crypto ipsec  
security-  
association lifetime  
kilobytes 4608000  
**crypto dynamic-map DYN 10 set transform-set TRA**  
crypto map MAP 65000  
ipsec-isakmp dynamic  
DYN  
crypto map MAP  
interface outside

24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Предложение # 12 по КОНТЕКСТУ БЕЗОПАСНОСТИ IPSEC, Преобразовывает глобальную запись # 10 КОНТЕКСТА БЕЗОПАСНОСТИ IPSEC # 1 acceptableMatches  
24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, IKE: запрос SPI!  
IPSec: Новый начальный SA, созданный 0xcfdffc90, SCB: 0xCFDFFB58, Направление: входящий SPI: 0x9E18ACB2  
Идентификатор сеанса: 0x00138000  
Цифра VPIF: 0x00000004  
Тип туннеля: Ra  
Протокол: особенно  
Срок действия: 240 секунд  
24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, IKE получил SPI от ключевого механизма: SPI = 0x9e18acb2  
24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, oakley построение быстрого режима  
24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, создавая пробел хеширует информационное наполнение  
24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, создавая информационное наполнение КОНТЕКСТА БЕЗОПАСНОСТИ IPSEC  
24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Отвергая продолжительность смены ключа IPSec Инициатора от 2147483 до 86400 секунд  
24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, создавая информационное наполнение параметра IPSec  
24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, создавая Proxy Id  
24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Передавая Proxy Id:  
Удаленный хост: 192.168.1.100Protocol 0Port 0  
Локальный subnet:0.0.0.0mask 0.0.0.0 Протокола 0Port 0  
24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Передача уведомления СРОКА ДЕЙСТВИЯ РЕСПОНДЕНТА Инициатору

	24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, создавая qm хеширует информационное наполнение	
Передайте QM2.	24 августа 11:31:13 [IKEv1 ДЕКОДИРУЕТ] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Респондент IKE, передающий 2-й QM PKT: идентификатор сообщения = 0e83792e 24 августа 11:31:13 [IKEv1] IP = 64.102.156.87, сообщение (msgid=e83792e) ПЕРЕДАЧИ IKE_DECODE с информационными наполнениями: HDR + ХЭШ (8) + SA (1) + ПАРАМЕТР (10) + ID (5) + ID (5) + УВЕДОМЛЯЕТ (11) + NONE (0) общая длина: 184	
	<b>===== Сообщение 2 (QM2) Быстрого режима =====&gt;</b>	
	60811:28:39.96208/24/12Sev=Info/4IKE/0x63000014 ПОЛУЧАЯ <<<QM ISAKMP OAK * (ХЭШ, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) от 64.102.156.88	Получите QM2.
	60911:28:39.96408/24/12Sev=Decode/11IKE/0x63000001 1 Заголовок ISAKMP Инициатор COOKIE:D56197780D7BE3E5 Респондент COOKIE:1B301D2DE710EDA0 Следующий Payload:Hash Ver (Hex):10 Exchange режим Type:Quick Flags:(Encryption) MessageID (Hex): E83792E Длина: 188 Хэш информационного наполнения Следующее информационное наполнение: сопоставление безопасности Зарезервированный: 00 Длина полезных данных: 24 Данные (в Hex): CABF38A62C9B88D1691E81F3857D6189534B2EC0 Сопоставление безопасности информационного наполнения Следующее информационное наполнение: параметр Зарезервированный: 00 Длина полезных данных: 52 DOI: IPSec Ситуация: (SIT_IDENTITY_ONLY)  Предложение по информационному наполнению Следующее информационное наполнение: Нет Зарезервированный: 00 Длина полезных данных: 40 Proposal 1 Идентификатор протокола: PROTO_IPSEC_ESP Размер SPI: 4 # преобразований: 1 SPI: 9E18ACB2	Процесс QM2. Дешифрованное информационное наполнение показывает выбранные предложения.

	<p>Информационное наполнение преобразовывает  Следующее информационное наполнение: Нет  Зарезервированный: 00  Длина полезных данных: 28  Преобразуйте #: 1  Преобразовывать-идентификатор: ESP_3DES  Reserved2: 0000  Тип жизни: секунды  Срок службы (Hex): 0020C49B  Режим инкапсуляции: туннель UDP  Алгоритм аутентификации: SHA1  Параметр информационного наполнения  Следующее информационное наполнение:  идентификация  Зарезервированный: 00  Длина полезных данных: 24  Данные (в Hex):  3A079B75DA512473706F235EA3FCA61F1D15D4CD  Идентификация информационного наполнения  Следующее информационное наполнение:  идентификация  Зарезервированный: 00  Длина полезных данных: 12  ID Type: Адрес IPv4  Идентификатор протокола (UDP/TCP, и т.д.): 0  Порт: 0  ID Data; 192.168.1.100  Идентификация информационного наполнения  Следующее информационное наполнение:  уведомление  Зарезервированный: 00  Длина полезных данных: 16  ID Type: Подсеть IPv4  Идентификатор протокола (UDP/TCP, и т.д.): 0  Порт: 0  ID Data; 0.0.0.0/0.0.0.0  Уведомление информационного наполнения  Следующее информационное наполнение: Нет  Зарезервированный: 00  Длина полезных данных: 28  DOI: IPSec  Идентификатор протокола: PROTO_IPSEC_ESP  Размер Spi: 4  Уведомьте тип: STATUS_RESP_LIFETIME  SPI: 9E18ACB2  Data;  Тип жизни: секунды  Срок службы (Hex): 00015180</p>	
	<p>61011:28:39.96508/24/12Sev=Debug/7IKE/0x63000076  Трассировка NAV-&gt; QM:MsgID=0E83792ECurState:  QM_WAIT_MSG2Event: EV_RCVD_MSG  61111:28:39.96508/24/12Sev=Info/5IKE/0x63000045</p>	<p>Процесс QM2.</p>



	<p>СРОК ДЕЙСТВИЯ РЕСПОНДЕНТА уведомляет, имеет значение 86400 секунд  61211:28:39.96508/24/12Sev=Debug/7IKE/0x63000076  Трассировка NAV-&gt; QM:MsgID=0E83792ECurState:  QM_WAIT_MSG2Event: EV_CHK_PFS  61311:28:39.96508/24/12Sev=Debug/7IKE/0x63000076</p>	
	<p>Трассировка NAV-&gt; QM:MsgID=0E83792ECurState:  QM_BLD_MSG3Event: EV_BLD_MSG  61411:28:39.96508/24/12Sev=Debug/7IKE/0x63000076  Заголовок ISAKMP  Инициатор COOKIE:D56197780D7BE3E5  Респондент COOKIE:1B301D2DE710EDA0  Следующий Payload:Hash  Ver (Hex):10  Exchange режим Type:Quick  Flags:(Encryption)  MessageID (Hex): E83792E  Длина: 52</p> <p>Хэш информационного наполнения  Следующее информационное наполнение: Нет  Зарезервированный: 00  Длина полезных данных: 24  Данные (в Hex):  CDDC20D91EB4B568C826D6A5770A5CF020141236</p>	<p>Создайте QM3.  Дешифрованное информационное наполнение для QM3, показанного здесь. Этот процесс includes хэш.</p>
	<p>61511:28:39.96508/24/12Sev=Debug/7IKE/0x63000076  Трассировка NAV-&gt; QM:MsgID=0E83792ECurState:  QM_SND_MSG3Event: EV_SND_MSG  61611:28:39.96508/24/12Sev=Info/4IKE/0x63000013  ПЕРЕДАЧА&gt;&gt;&gt; QM ISAKMP OAK * (ХЭШ) к  64.102.156.88</p>	<p>Передайте QM3.  Клиент теперь готов зашифровать и дешифровать.</p>
	<p><b>&lt;===== сообщение 3 (QM3) быстрого режима =====&gt;</b></p>	
Получите QM3.	<p>24 августа 11:31:13 [IKEv1] IP = 64.102.156.87,  IKE_DECODE ПОЛУЧИЛ сообщение (msgid=e83792e)  с информационными наполнениями: HDR + ХЭШ (8) +  NONE (0) общая длина: 52</p>	
Процесс QM3. Создайте (SPI) индексов параметра безопасности входящего и исходящего трафика. Добавьте статический маршрут для хоста. Соответствующая конфигурация: crypto ipsec transform-set TRA esp-aes esp-sha-hmac	<p>24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec,  Имя пользователя = user1, IP = 64.102.156.87,  обрабатывая информационное наполнение хэша  24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec,  Имя пользователя = user1, IP = 64.102.156.87,  загружая все КОНТЕКСТЫ БЕЗОПАСНОСТИ IPSEC  24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec,  Имя пользователя = user1, IP = 64.102.156.87,  Генерируя Ключ Быстрого режима!  24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec,  Имя пользователя = user1, IP = 64.102.156.87, NP  шифрует поиск правила для криптокарты out-dyn-map  10 соответствующий Неизвестный ACL:  возвращенный  cs_id=cc107410; rule=00000000  24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec,</p>	

```
crypto ipsec
security-
association lifetime
seconds 28800
crypto ipsec
security-
association lifetime
kilobytes 4608000
crypto dynamic-map
DYN 10 set transform-
set TRA
crypto dynamic-map
DYN 10 set reverse-
route
```

Имя пользователя = user1, IP = 64.102.156.87,  
Генерируя Ключ Быстрого режима!  
IPSec: Новый начальный SA, созданный 0xccc9ed60,  
SCB: 0xCF7F59E0,  
Направление: исходящий  
SPI: 0xC055290A  
Идентификатор сеанса: 0x00138000  
Цифра VPIF: 0x00000004  
Тип туннеля: Ра  
Протокол: особенно  
Срок действия: 240 секунд  
IPSec: Завершенный хост обновление OBSA, SPI  
0xC055290A  
IPSec: Создавая исходящий контекст VPN, SPI  
0xC055290A  
Флаги: 0x00000025  
SA: 0xccc9ed60  
SPI: 0xC055290A  
MTU: 1500 байтов  
VCID: 0x00000000  
Одноранговый узел: 0x00000000  
SCB: 0xA5922B6B  
Канал: 0xc82afb60  
IPSec: Завершенный исходящий контекст VPN, SPI  
0xC055290A  
Маркер VPN: 0x0015909c  
IPSec: Новый исходящий шифруют правило, SPI  
0xC055290A  
Адрес src: 0.0.0.0  
Маска src: 0.0.0.0  
Адрес dst: 192.168.1.100  
Маска dst: 255.255.255.255  
Порты src  
Верхний: 0  
Ниже: 0  
Op: игнорировать  
Порты dst  
Верхний: 0  
Ниже: 0  
Op: игнорировать  
Протокол: 0  
Протокол использования: FALSE  
SPI: 0x00000000  
SPI использования: FALSE  
IPSec: Завершенный исходящий шифруют правило,  
SPI 0xC055290A  
ID правила: 0xcb47a710  
IPSec: Новое исходящее правило разрешения, SPI  
0xC055290A  
Адрес src: 64.102.156.88  
Маска src: 255.255.255.255  
Адрес dst: 64.102.156.87  
Маска dst: 255.255.255.255

Порты src  
Верхний: 4500  
Ниже: 4500  
Ор: равный  
Порты dst  
Верхний: 58506  
Ниже: 58506  
Ор: равный  
Протокол: 17  
Протокол использования: tTRUE  
SPI: 0x00000000  
SPI использования: fALSE  
IPSec: Завершенное исходящее правило разрешения,  
SPI 0xC055290A  
ID правила: 0xcdf3cfa0  
24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec,  
Имя пользователя = user1, IP = 64.102.156.87, NP  
шифрует поиск правила для криптокарты out-dyn-map  
10 соответствующий Неизвестный ACL:  
возвращенный  
cs\_id=cc107410; rule=00000000  
24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя  
пользователя = user1, IP = 64.102.156.87,  
Согласование безопасности завершает для  
Пользователя (user1) Респондента, Входящий SPI =  
0x9e18acb2, Исходящий  
SPI = 0xc055290a  
24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec,  
Имя пользователя = user1, IP = 64.102.156.87, IKE  
получил сообщение KEY\_ADD для SA: SPI =  
0xc055290a  
IPSec: Завершенный хост обновление IBSA, SPI  
0x9E18ACB2  
IPSec: Создавая входящий контекст VPN, SPI  
0x9E18ACB2  
Флаги: 0x00000026  
SA: 0xcdfffc90  
SPI: 0x9E18ACB2  
MTU: 0 байтов  
VCID: 0x00000000  
Одноранговый узел: 0x0015909C  
SCB: 0xA5672481  
Канал: 0xc82afb60  
IPSec: Завершенный входящий контекст VPN, SPI  
0x9E18ACB2  
Маркер VPN: 0x0016219c  
IPSec: Обновляя исходящий контекст VPN  
0x0015909C, SPI 0xC055290A  
Флаги: 0x00000025  
SA: 0xc9ed60  
SPI: 0xC055290A  
MTU: 1500 байтов  
VCID: 0x00000000

Одноранговый узел: 0x0016219C  
SCB: 0xA5922B6B  
Канал: 0xc82afb60  
IPSec: Завершенный исходящий контекст VPN, SPI  
0xC055290A  
Маркер VPN: 0x0015909c  
IPSec: Завершенное исходящее внутреннее правило,  
SPI 0xC055290A  
ID правила: 0xcb47a710  
IPSec: Завершенное исходящее внешнее правило  
SPD, SPI 0xC055290A  
ID правила: 0xcdf3cfa0  
IPSec: Новый входящий туннель течет правило, SPI  
0x9E18ACB2  
Адрес src: 192.168.1.100  
Маска src: 255.255.255.255  
Адрес dst: 0.0.0.0  
Маска dst: 0.0.0.0  
Порты src  
Верхний: 0  
Ниже: 0  
Op: игнорировать  
Порты dst  
Верхний: 0  
Ниже: 0  
Op: игнорировать  
Протокол: 0  
Протокол использования: FALSE  
SPI: 0x00000000  
SPI использования: FALSE  
IPSec: Завершенный входящий туннель течет  
правило, SPI 0x9E18ACB2  
ID правила: 0xcdf15270  
IPSec: Новый входящий дешифруют правило, SPI  
0x9E18ACB2  
Адрес src: 64.102.156.87  
Маска src: 255.255.255.255  
Адрес dst: 64.102.156.88  
Маска dst: 255.255.255.255  
Порты src  
Верхний: 58506  
Ниже: 58506  
Op: равный  
Порты dst  
Верхний: 4500  
Ниже: 4500  
Op: равный  
Протокол: 17  
Протокол использования: TRUE  
SPI: 0x00000000  
SPI использования: FALSE  
IPSec: Завершенный входящий дешифруют правило,  
SPI 0x9E18ACB2

	<p>ID правила: 0xc03c2f8  IPSec: Новое входящее правило разрешения, SPI 0x9E18ACB2  Адрес src: 64.102.156.87  Маска src: 255.255.255.255  Адрес dst: 64.102.156.88  Маска dst: 255.255.255.255  Порты src  Верхний: 58506  Ниже: 58506  Ор: равный  Порты dst  Верхний: 4500  Ниже: 4500  Ор: равный  Протокол: 17  Протокол использования: tRUE  SPI: 0x00000000  SPI использования: fALSE  IPSec: Завершенное входящее правило разрешения, SPI 0x9E18ACB2  ID правила: 0xc6f58c0  24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Питчер: полученный KEY_UPDATE, spi 0x9e18acb2  24 августа 11:31:13 [IKEv1 DEBUG] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Запуская P2 повторно вводит таймер: 82080 секунд.  24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, Добавляя статический маршрут для адреса клиента: 192.168.1.100</p>	
<p>Завершенная фаза 2. Обе стороны шифруют и дешифруют теперь.</p>	<p>24 августа 11:31:13 [IKEv1] Группа = ipsec, Имя пользователя = user1, IP = 64.102.156.87, ФАЗА 2 ЗАВЕРШИЛА (msgid=0e83792e)</p>	
<p>Для аппаратных клиентов получено еще одно сообщение, куда клиент передает информацию о себе. Если вы смотрите тщательно, необходимо найти имя хоста Клиента EzVPN, программное обеспечение, которое выполнено на клиенте, и местоположении и</p>	<p>24 августа 11:31:13 [IKEv1]: IP = 10.48.66.23, IKE_DECODE ПОЛУЧИЛ сообщение (msgid=91facc9) с информационными наполнениями: HDR + ХЭШ (8) + УВЕДОМЛЯЕТ (11) + NONE (0) общая длина: 184  24 августа 11:31:13 [IKEv1 DEBUG]: Группа = EZ, Имя пользователя = Cisco, IP = 10.48.66.23, обрабатывая информационное наполнение хэша  24 августа 11:31:13 [IKEv1 DEBUG]: Группа = EZ, Имя пользователя = Cisco, IP = 10.48.66.23, обработка уведомляет информационное наполнение  24 августа 11:31:13 [IKEv1 ДЕКОДИРУЕТ]: ДЕСКРИПТОР OBSOLETE - ИНДЕКС 1  24 августа 11:31:13 [IKEv1 ДЕКОДИРУЕТ]: 0000: 00000000 7534000B 62736E73 2D383731 .... u4.. bsns-871 0010: 2D332E75 32000943 6973636F 20383731 -</p>	

<p>названии программного обеспечения</p>	<p><b>3.u2.. Cisco 871</b>  0020: 7535000B 46484B30 39343431 32513675 u5..  FHK094412Q6u  0030: 36000932 32383538 39353638 75390009 6..  228589568u9..  0040: 31343532 31363331 32753300  2B666C61 145216312u3. + <b>fla</b>  0050: 73683A63 3837302-й 61647669  70736572 <b>sh:c870-advipser</b>  0060: 76696365 736B392D 6D7A2E31  32342D32 <b>vicesk9-mz.124-2</b>  0070: 302E5435 2E62696E <b>0. T5.bin</b></p> <p>24 августа 11:31:13 [IKEv1 DEBUG]: Группа = EZ, Имя  пользователя = Cisco, IP = 10.48.66.23, Обработывая  Хэш PSK  24 августа 11:31:13 [IKEv1]: Группа = EZ, Имя  пользователя = Cisco, IP = 192.168.1.100,  Противоречивый размер хэша PSK  24 августа 11:31:13 [IKEv1 DEBUG]: Группа = EZ, Имя  пользователя = Cisco, IP = 10.48.66.23, Отказавшая  Проверка Хэша PSK!</p>	
--	---	--

## Туннельная проверка

### ISAKMP

Выходные данные от крика **sh isa sa det** команда:

```
crypto ipsec transform-
set TRA esp-aes esp-
sha-hmac
crypto ipsec security-
association lifetime
seconds 28800
crypto ipsec security-
association lifetime
kilobytes 4608000
crypto dynamic-map
DYN 10 set transform-
set TRA
crypto dynamic-map
DYN 10 set reverse-
route
```

### IPSec

Так как Протокол ICMP используется для инициирования туннеля, только один контекст безопасности IPSec подключен. Протокол 1 является ICMP. Обратите внимание на то, что значения SPI отличаются от тех, о которых выполняют согласование в отладках. Это - фактически, тот же туннель после того, как Фаза 2 повторно введет.

Выходные данные от `sh крипто-ipsec sa` команда:

```
crypto ipsec transform-  
set TRA esp-aes esp-  
sha-hmac  
crypto ipsec security-  
association lifetime  
seconds 28800  
crypto ipsec security-  
association lifetime  
kilobytes 4608000  
crypto dynamic-map  
DYN 10 set transform-  
set TRA  
crypto dynamic-map  
DYN 10 set reverse-  
route
```

## Дополнительные сведения

- [Статья Википедии относительно IPsec](#)
- [Устранение неполадок IPsec - общие сведения и использование команд debug](#)
- [Cisco Systems – техническая поддержка и документация](#)