ASA IPsec and IKE Debugs (IKEv1 Aggressive Mode) Troubleshooting Tech Note

Contents

Introduction

This document describes debugs on the Cisco Adaptive Security Appliance (ASA) when both aggressive mode and pre-shared key (PSK) are used. The translation of certain debug lines into configuration is also discussed. Cisco recommends you have a basic knowledge of IPsec and Internet Key Exchange (IKE).

This document does not discuss passing traffic after the tunnel has been established.

Core Issue

IKE and IPsec debugs are sometimes cryptic, but you can use them in order to understand problems with IPsec VPN tunnel establishment.

Scenario

Aggressive mode is typically used in case of Easy VPN (EzVPN) with software (Cisco VPN Client) and hardware clients (Cisco ASA 5505 Adaptive Security Appliance or Cisco IOS® Software routers), but only when a pre-shared key is used. Unlike main mode, aggressive mode consists of three messages.

The debugs are from an ASA that runs software version 8.3.2 and acts as an EzVPN server. The

EzVPN client is a software client.

debug Commands Used

These are the debug commands used in this document:

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

ASA Configuration

The ASA configuration in this example is meant to be strictly basic; no external servers are used.

```
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
```

Debugging

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Server Message Description	Debugs	Client Message Description
	49711:28:30.28908/24/12Sev=Info/6IKE/0x6300003B Attempting to establish a connection with 64.102.156.88. 49811:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_INITIALEvent: EV_INITIATOR 49911:28:30.29708/24/12Sev=Info/4IKE/0x63000001 Starting IKE Phase 1 Negotiation 50011:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_GEN_DHKEY 50111:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_BLD_MSG 50211:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_START_RETRY_TMR 50311:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_SND_MSG	Aggressive mode starts. Construct AM1. This process includes: - ISAKMP HDR - Security appliance (SA) that contains all transform payloads and proposals supported by the client - Key Exchange payload - Phase 1 initiator ID - Nonce
	50411:28:30.30408/24/12Sev=Info/4IKE/0x63000013 SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID(Xauth), VID(dpd), VID(Frag), VID(Nat-T), VID(Unity)) to 64.102.156.88	Send AM1.
	<========== Aggressive Message 1 (AM1) ==========	
Receive AM1 from client.	Aug 24 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA (1)	50611:28:30.33308/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_WAIT_MSG2Event: EV_NO_EVENT	Wait for response from server.

	+ KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 849		

Process AM1. Compare received proposals and transforms with those already configured for matches.
Relevant configuration:
ISAKMP is enabled on interface, and at least one policy is defined that matches what the client sent:
`crypto isakmp enable outside`
`crypto isakmp policy 10`
`authentication pre-share`
`encryption aes`
`hash sha`
`group 2`
`lifetime 86400`
Tunnel-group matching the identity name present:
`tunnel-group EZ type remote-access`
`tunnel-group EZ general-attributes`
`default-group-policy EZ`
`tunnel-group EZ ipsec-attributes`
`pre-shared-key cisco`
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, processing SA payload
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, processing ke payload
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, processing ISA_KE payload
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, processing nonce payload
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, processing ID payload
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, processing VID payload
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Received xauth V6 VID
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, processing VID payload
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Received DPD VID
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, processing VID payload
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Received Fragmentation VID
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, IKE Peer included IKE fragmentation capability flags: Main Mode:TrueAggressive Mode:False
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, processing VID payload
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Received NAT-Traversal ver 02 VID
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, processing VID payload
	Aug 24 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Received Cisco Unity client VID
	Aug 24 11:31:03 [IKEv1]IP = 64.102.156.87, Connection landed on tunnel_group ipsec
	Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, processing IKE SA payload
	Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5	

	Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1]Phase 1 failure:Mismatched attribute types for class Group Description:Rcv'd: Group 2Cfg'd: Group 5 Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, IKE SA Proposal # 1, Transform # 5 acceptableMatches global IKE entry # 1	
Construct AM2. This process includes: - chosen policies - Diffie-Hellman (DH) - Responder ID	Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing ISAKMP SA payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing ke payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP =	

- auth - Network Address Translation (NAT) detection payload	64.102.156.87, constructing nonce payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Generating keys for Responder... Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing ID payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing hash payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Computing hash for ISAKMP Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing Cisco Unity VID payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing xauth V6 VID payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing dpd vid payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing NAT-Traversal VID ver 02 payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing NAT-Discovery payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, computing NAT Discovery hash Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing NAT-Discovery payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, computing NAT Discovery hash Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing Fragmentation VID + extended capabilities payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing VID payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Send Altiga/Cisco VPN3000/Cisco ASA GW VID	
Send AM2.	Aug 24 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 444	
	========== Aggressive Message 2 (AM2) ==========>	
	50711:28:30.40208/24/12Sev=Info/5IKE/0x6300002F Received ISAKMP packet: peer = 64.102.156.8 50811:28:30.40308/24/12Sev=Info/4IKE/0x63000014 RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID(Unity), VID(Xauth), VID(dpd), VID(Nat-T), NAT-D, NAT-D, VID(Frag), VID(?)) from 64.102.156.88 51011:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState:	Receive AM2.

	AM_WAIT_MSG2Event: EV_RCVD_MSG	
	51111:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Peer is a Cisco-Unity compliant peer 51211:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Peer supports XAUTH 51311:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Peer supports DPD 51411:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Peer supports NAT-T 51511:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Peer supports IKE fragmentation payloads 51611:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_GEN_SKEYID 51711:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_AUTHENTICATE_PEER 51811:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_ADJUST_PORT 51911:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_CRYPTO_ACTIVE	Process AM 2.
	52011:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Event: EV_BLD_MSG] 52111:28:30.42208/24/12Sev=Debug/8IKE/0x63000001 IOS Vendor ID Contruction started 52211:28:30.42208/24/12Sev=Info/6IKE/0x63000001 IOS Vendor ID Contruction successful	Construct AM3. This process includes Client Auth. At this point all data relevant for encryption has already been exchanged.
	52311:28:30.42308/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Event: EV_SND_MSG 52411:28:30.42308/24/12Sev=Info/4IKE/0x63000013 SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT, NAT-D, NAT-D, VID(?), VID(Unity)) to 64.102.156.88	Send AM3.
	<========== Aggressive Message 3 (AM3)	

	==========	
Receive AM3 from client.	Aug 24 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + HASH (8) + NOTIFY (11) + NAT-D (130) + NAT-D (130) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 168	
Process AM 3. Confirm NAT traversal (NAT-T) use. Both sides are now ready to start traffic encryption.	Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, processing hash payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Computing hash for ISAKMP Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, processing notify payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, processing NAT-Discovery payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, computing NAT Discovery hash Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, processing NAT-Discovery payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, computing NAT Discovery hash Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, processing VID payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Processing IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000408) Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, processing VID payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Received Cisco Unity client VID Aug 24 11:31:03 [IKEv1]Group = ipsec, IP = 64.102.156.87, Automatic NAT Detection Status:Remote endISbehind a NAT deviceThisend is NOT behind a NAT device	
Initiate Phase 1.5 (XAUTH), and request user credentials.	Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing blank hash payload Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, constructing qm hash payload Aug 24 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Message (msgid=fb709d4d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 72	
	========== XAuth - Credentials Request ==========>	
	53511:28:30.43008/24/12Sev=Info/4IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 64.102.156.88 53611:28:30.43108/24/12Sev=Decode/11IKE/0x63000001 ISAKMP Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Next Payload:Hash Ver (Hex):10	Receive Auth request. Decrypted payload shows empty username and password fields.

	Exchange Type:Transaction Flags:(Encryption) MessageID(Hex):FB709D4D Length:76 Payload Hash Next Payload: Attributes Reserved: 00 Payload Length: 24 Data (In Hex): C779D5CBC5C75E3576C478A15A7CAB8A83A232D0 Payload Attributes Next Payload: None Reserved: 00 Payload Length: 20 Type: ISAKMP_CFG_REQUEST Reserved: 00 Identifier: 0000 XAUTH Type: Generic XAUTH User Name: (empty) XAUTH User Password: (empty) 53711:28:30.43108/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_INITIALEvent: EV_RCVD_MSG	
	53811:28:30.43108/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent: EV_INIT_XAUTH 53911:28:30.43108/24/12 Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent: EV_START_RETRY_TMR 54011:28:30.43208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_NO_EVENT 541 11:28:36.41508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_RCVD_USER_INPUT	Initiate Phase 1.5 (XAUTH). Initiate retry timer as it awaits user input. When retry timer runs out, connection is automatically disconnected.
	54211:28:36.41508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_SND_MSG 54311:28:36.41508/24/12Sev=Info/4IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 64.102.156.88 54411:28:36.41508/24/12Sev=Decode/11IKE/0x63000001 ISAKMP Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0	Once user input is received, send user credentials to the server. Decrypted payload shows filled (but hidden) username and

	Next Payload:Hash Ver (Hex):10 Exchange Type:Transaction Flags:(Encryption) MessageID(Hex):FB709D4D Length:85 Payload Hash Next Payload: Attributes Reserved: 00 Payload Length: 24 Data (In Hex): 1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5 Payload Attributes Next Payload: None Reserved: 00 Payload Length: 33 Type: ISAKMP_CFG_REPLY Reserved: 00 Identifier: 0000 XAUTH Type: Generic XAUTH User Name: (data not displayed) XAUTH User Password: (data not displayed)	password fields. Send mode config request (various attributes).
	<========== Xauth - User Credentials ==========	
Receive user credentials.	Aug 24 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=fb709d4d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 85 Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, process_attr(): Enter!	
Process user credentials. Verify credentials, and generate mode config payload. Relevant configuration: `username cisco password cisco`	Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Processing MODE_CFG Reply attributes. Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: primary DNS = 192.168.1.99 Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: secondary DNS = cleared Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: primary WINS = cleared Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: secondary WINS = cleared Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: split tunneling list = split Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: default domain = jyoungta-labdomain.cisco.com	

	Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: IP Compression = disabled Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: Split Tunneling Policy = Disabled Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: Browser Proxy Setting = no-modify Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: Browser Proxy Bypass Local = disable Aug 24 11:31:09 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, User (user1) authenticated.	
Send xuath result.	Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, constructing blank hash payload Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, constructing qm hash payload Aug 24 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Message (msgid=5b6910ff) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 64	
	========== XAuth - Authorization Result ==========>	
	54511:28:36.41608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_XAUTHREQ_DONE 54611:28:36.41608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_NO_EVENT 54711:28:36.42408/24/12Sev=Info/5IKE/0x6300002F Received ISAKMP packet: peer = 64.102.156.88 54811:28:36.42408/24/12Sev=Info/4IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 64.102.156.88 54911:28:36.42508/24/12Sev=Decode/11IKE/0x63000001 ISAKMP Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Next Payload:Hash Ver (Hex):10 Exchange Type:Transaction Flags:(Encryption) MessageID(Hex):5B6910FF	Receive auth results, and process results.

	Length:76 Payload Hash Next Payload: Attributes Reserved: 00 Payload Length: 24 Data (In Hex): 7DCF47827164198731639BFB7595F694C9DDFE85 Payload Attributes Next Payload: None Reserved: 00 Payload Length: 12 Type: ISAKMP_CFG_SET Reserved: 00 Identifier: 0000 XAUTH Status: Pass 55011:28:36.42508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_INITIALEvent: EV_RCVD_MSG 55111:28:36.42508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_INIT_XAUTH 55211:28:36.42508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_CHK_AUTH_RESULT	
	55311:28:36.42508/24/12Sev=Info/4IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 64.102.156.88	ACK result.
	<========== Xauth - Acknowledgement ==========	
Receive and process ACK; no response from server.	Aug 24 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=5b6910ff) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60 Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, process_attr(): Enter! Aug 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Processing cfg ACK attributes	
	55511:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_XAUTH_DONE_SUC 55611:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_NO_EVENT 55711:28:36.42608/24/12Sev=Debug/7IKE/0x6300007	Generate mode-config request. Decrypted payload shows requested parameters from server.

	6 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_TERM_REQUEST 55811:28:36.42608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_REMOVE 55911:28:36.42608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_NO_EVENT 56011:28:36.42608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_XAUTH_PROGEvent: EV_XAUTH_DONE_SUC 56111:28:38.40608/24/12Sev=Debug/8IKE/0x6300004 C Starting DPD timer for IKE SA (I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0) sa->state = 1, sa- >dpd.worry_freq(mSec) = 5000 56211:28:38.40608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_MODECFG 56311:28:38.40608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_NO_EVENT 56411:28:38.40608/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=84B4B653CurState: TM_INITIALEvent: EV_INIT_MODECFG 56511:28:38.40808/24/12Sev=Info/5IKE/0x6300005E Client sending a firewall request to concentrator 56611:28:38.40908/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_START_RETRY_TMR	
	56711:28:38.40908/24/12Sev=Debug/7IKE/0x6300007 6 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_SND_MSG 56811:28:38.40908/24/12Sev=Info/4IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 64.102.156.88 56911:28:38.62708/24/12Sev=Decode/11IKE/0x63000 001 ISAKMP Header	Send mode-config request.

	Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Next Payload:Hash Ver (Hex):10 Exchange Type:Transaction Flags:(Encryption) MessageID(Hex):84B4B653 Length:183 Payload Hash Next Payload: Attributes Reserved: 00 Payload Length: 24 Data (In Hex): 81BFBF6721A744A815D69A315EF4AAA571D6B687 Payload Attributes Next Payload: None Reserved: 00 Payload Length: 131 Type: ISAKMP_CFG_REQUEST Reserved: 00 Identifier: 0000 IPv4 Address: (empty) IPv4 Netmask: (empty) IPv4 DNS: (empty) IPv4 NBNS (WINS): (empty) Address Expiry: (empty) Cisco extension: Banner: (empty) Cisco extension: Save PWD: (empty) Cisco extension: Default Domain Name: (empty) Cisco extension: Split Include: (empty) Cisco extension: Split DNS Name: (empty) Cisco extension: Do PFS: (empty) Unknown: (empty) Cisco extension: Backup Servers: (empty) Cisco extension: Smart Card Removal Disconnect: (empty) Application Version: Cisco Systems VPN Client 5.0.07.0290:WinNT Cisco extension: Firewall Type: (empty) Cisco extension: Dynamic DNS Hostname: ATBASU-LABBOX		
	<========== Mode-config Request ==========		
Receive mode-config request.	Aug 24 11:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message	57011:28:38.62808/24/12Sev= Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_NO_EVENT	Wait for server response.

	(msgid=84b4b653) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 183 Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, process_attr(): Enter!		
Process mode-config request. Many of these values are usually configured in the group-policy. However, since the server in this example has a very basic configuration, you do not see them here.	Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Processing cfg Request attributes Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for IPV4 address! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for IPV4 net mask! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for DNS server address! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for WINS server address! Aug 24 11:31:11 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Received unsupported transaction mode attribute: 5 Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for Banner! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for Save PW setting! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for Default Domain Name! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for Split Tunnel List! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for Split DNS! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG:	

	Received request for PFS setting! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for Client Browser Proxy Setting! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for backup ip-sec peer list! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for Client Smartcard Removal Disconnect Setting! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for Application Version! Aug 24 11:31:11 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Client Type: WinNTClient Application Version: 5.0.07.0290 Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for FWTYPE! Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Received request for DHCP hostname for DDNS is: ATBASU-LABBOX!	

Construct mode-config response with all values that are configured.
Relevant configuration:
Note in this case, the user is always assigned the same IP.
`username cisco 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`
	Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Obtained IP addr (192.168.1.100) prior to initiating Mode Cfg (XAuth enabled)
	Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Sending subnet mask (255.255.255.0) to remote client
	Aug 24 11:31:11 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Assigned private IP address 192.168.1.100 to remote user
	Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, constructing blank hash payload
	Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, construct_cfg_set: default domain = jyoungta-labdomain.cisco.com
	Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Send Client Browser Proxy Attributes!
	Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Browser Proxy set to No-Modify. Browser Proxy data will NOT be included in the mode-cfg reply
	Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Send Cisco Smartcard Removal Disconnect enable!!
	Aug 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, constructing	

	qm hash payload		
Send mode-config response.	Aug 24 11:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Message (msgid=84b4b653) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 215		
	========== Mode-config Response ==========>		
	57111:28:38.63808/24/12Sev=Info/5IKE/0x6300002F Received ISAKMP packet: peer = 64.102.156.88 57211:28:38.63808/24/12Sev=Info/4IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 64.102.156.88 57311:28:38.63908/24/12Sev=Decode/11IKE/0x63000001 ISAKMP Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Next Payload:Hash Ver (Hex):10 Exchange Type:Transaction Flags:(Encryption) MessageID(Hex):84B4B653 Length:220 Payload Hash Next Payload: Attributes Reserved: 00 Payload Length: 24 Data (In Hex): 6DE2E70ACF6B1858846BC62E590C00A66745D14D Payload Attributes Next Payload: None Reserved: 00 Payload Length: 163 Type: ISAKMP_CFG_REPLY Reserved: 00 Identifier: 0000 IPv4 Address: 192.168.1.100 IPv4 Netmask: 255.255.255.0 IPv4 DNS: 192.168.1.99 Cisco extension: Save PWD: No Cisco extension: Default Domain Name: jyoungta-labdomain.cisco.com Cisco extension: Do PFS: No Application Version: Cisco Systems, Inc ASA5505 Version 8.4(4)1 built by builders on Thu 14-Jun-12 11:20 Cisco extension: Smart Card Removal Disconnect: Yes		Receive mode-config parameter values from server.
Phase 1 completes on server. Initiate quick mode (QM) process.	Aug 24 11:31:13 [IKEv1 DECODE]IP = 64.102.156.87, IKE	57411:28:38.63908/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_RCVD_MSG	Process parameters, and configure itself accordingly.

	Responder starting QM: msg id = 0e83792e Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Gratuitous ARP sent for 192.168.1.100 Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, PHASE 1 COMPLETED	57511:28:38.63908/24/12Sev= Info/5IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS:, value = 192.168.1.100 57611:28:38.63908/24/12Sev=Info/5IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK:, value = 255.255.255.0 57711:28:38.63908/24/12Sev= Info/5IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 192.168.1.99 57811:28:38.63908/24/12Sev=Info/5IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 57911:28:38.63908/24/12Sev=Info/5IKE/0x6300000E MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: , value = jyoungta-labdomain.cisco.com 58011:28:38.63908/24/12Sev= Info/5IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 58111:28:38.63908/24/12Sev=Info/5IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc ASA5505 Version 8.4(4)1 built by builders on Thu 14-Jun-12 11:20 58211:28:38.63908/24/12Sev= Info/5IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SMARTCARD_REMOVAL_DISCONNECT: , value = 0x00000001 58311:28:38.63908/24/12Sev= Info/5IKE/0x6300000D MODE_CFG_REPLY: Attribute = Received and using NAT-T port number , value = 0x00001194 58411:28:39.36708/24/12Sev= Debug/9IKE/0x63000093 Value for ini parameter EnableDNSRedirection is 1	

		58511:28:39.36708/24/12Sev= Debug/7IKE/0x63000076 NAV Trace- >TM:MsgID=84B4B653CurState: TM_MODECFG_DONEEvent: EV_MODECFG_DONE_SUC	
Construct and send DPD for client.	Aug 24 11:31:13 [IKEv1]IP = 64.102.156.87, Keep-alive type for this connection: DPD Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Starting P1 rekey timer: 82080 seconds. Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, sending notify message Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, constructing blank hash payload Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, constructing qm hash payload Aug 24 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Message (msgid=be8f7821) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 92	
	========== Dead Peer Detection (DPD) ==========>	
	58811:28:39.79508/24/12Sev=Debug/7IKE/0x63000015 intf_data: lcl=0x0501A8C0, mask=0x00FFFFFF, bcast=0xFF01A8C0, bcast_vra=0xFF07070A 58911:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_P2 59011:28:39.79508/24/12Sev=Info/4IKE/0x63000056 Received a key request from Driver: Local IP = 192.168.1.100, GW IP = 64.102.156.88, Remote IP = 0.0.0.0 59111:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_ACTIVEEvent: EV_NO_EVENT 59211:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_INITIALEvent: EV_INITIATOR 59311:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG1Event: EV_CHK_PFS 59411:28:39.79608/24/12Sev=Debug/7IKE/0x6300007	Initiate QM, Phase 2. Construct QM1. This process includes: - Hash - SA with all Phase 2 proposals supported by the client, tunnel type and encryption - Nonce - Client ID - Proxy IDs

	6 NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG1Event: EV_BLD_MSG 59511:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG1Event: EV_START_RETRY_TMR	
	59611:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG1Event: EV_SND_MSG 59711:28:39.79608/24/12Sev=Info/4IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 64.102.156.88	Send QM1.
	<========== Quick Mode Message 1 (QM1) ==========	
Receive QM1.	Aug 24 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=e83792e) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 1026	
Process QM1. Relevant configuration: `crypto dynamic-map DYN 10 set transform-set TRA`	Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, processing hash payload Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, processing SA payload Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, processing nonce payload Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, processing ID payload Aug 24 11:31:13 [IKEv1 DECODE]Group = ipsec, Username = user1, IP = 64.102.156.87, ID_IPV4_ADDR ID received 192.168.1.100 Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Received remote Proxy Host data in ID Payload:Address 192.168.1.100, Protocol 0, Port 0 Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, processing ID payload Aug 24 11:31:13 [IKEv1 DECODE]Group = ipsec, Username = user1, IP = 64.102.156.87, ID_IPV4_ADDR_SUBNET ID received--0.0.0.0--0.0.0.0 Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Received local IP Proxy Subnet data in ID Payload:Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0 Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, QM IsRekeyed old sa not found by addr	

	Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Static Crypto Map check, checking map = out-map, seq = 10... Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Static Crypto Map Check by-passed: Crypto map entry incomplete! Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Selecting only UDP-Encapsulated-Tunnel andUDP-Encapsulated-Transport modes defined by NAT-Traversal Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Selecting only UDP-Encapsulated-Tunnel andUDP-Encapsulated-Transport modes defined by NAT-Traversal Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE Remote Peer configured for crypto map: out-dyn-map Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, processing IPSec SA payload	

Construct QM2. Relevant configuration:
`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`
	Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IPSec SA Proposal # 12, Transform # 1 acceptableMatches global IPSec SA entry # 10
	Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE: requesting SPI!
	IPSEC: New embryonic SA created @ 0xcfdffc90, SCB: 0xCFDFFB58, Direction: inbound
	SPI: 0x9E18ACB2
	Session ID: 0x00138000
	VPIF num: 0x00000004
	Tunnel type: ra
	Protocol: esp
	Lifetime: 240 seconds
	Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE got SPI from key engine: SPI = 0x9e18acb2
	Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, oakley constructing quick mode
	Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, constructing blank hash payload
	Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, constructing IPSec SA payload
	Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Overriding Initiator's IPSec rekeying duration from 2147483 to 86400 seconds
	Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, constructing IPSec nonce payload
	Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec,	

	Username = user1, IP = 64.102.156.87, constructing proxy ID Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Transmitting Proxy Id: Remote host: 192.168.1.100Protocol 0Port 0 Local subnet:0.0.0.0mask 0.0.0.0 Protocol 0Port 0 Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Sending RESPONDER LIFETIME notification to Initiator Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, constructing qm hash payload	
Send QM2.	Aug 24 11:31:13 [IKEv1 DECODE]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE Responder sending 2nd QM pkt: msg id = 0e83792e Aug 24 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Message (msgid=e83792e) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 184	
	========== Quick Mode Message 2 (QM2) ==========>	
	60811:28:39.96208/24/12Sev=Info/4IKE/0x63000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 64.102.156.88	Receive QM2.
	60911:28:39.96408/24/12Sev=Decode/11IKE/0x63000001 ISAKMP Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Next Payload:Hash Ver (Hex):10 Exchange Type:Quick Mode Flags:(Encryption) MessageID(Hex):E83792E Length:188 Payload Hash Next Payload: Security Association Reserved: 00 Payload Length: 24 Data (In Hex): CABF38A62C9B88D1691E81F3857D6189534B2EC0 Payload Security Association Next Payload: Nonce Reserved: 00 Payload Length: 52 DOI: IPsec Situation: (SIT_IDENTITY_ONLY) Payload Proposal	Process QM2. Decrypted payload shows chosen proposals.

	Next Payload: None Reserved: 00 Payload Length: 40 Proposal #: 1 Protocol-Id: PROTO_IPSEC_ESP SPI Size: 4 # of transforms: 1 SPI: 9E18ACB2 Payload Transform Next Payload: None Reserved: 00 Payload Length: 28 Transform #: 1 Transform-Id: ESP_3DES Reserved2: 0000 Life Type: Seconds Life Duration (Hex): 0020C49B Encapsulation Mode: UDP Tunnel Authentication Algorithm: SHA1 Payload Nonce Next Payload: Identification Reserved: 00 Payload Length: 24 Data (In Hex): 3A079B75DA512473706F235EA3FCA61F1D15D4CD Payload Identification Next Payload: Identification Reserved: 00 Payload Length: 12 ID Type: IPv4 Address Protocol ID(UDP/TCP, etc...): 0 Port: 0 ID Data: 192.168.1.100 Payload Identification Next Payload: Notification Reserved: 00 Payload Length: 16 ID Type: IPv4 Subnet Protocol ID(UDP/TCP, etc...): 0 Port: 0 ID Data: 0.0.0.0/0.0.0.0 Payload Notification Next Payload: None Reserved: 00 Payload Length: 28 DOI: IPsec Protocol-ID: PROTO_IPSEC_ESP Spi Size: 4 Notify Type: STATUS_RESP_LIFETIME SPI: 9E18ACB2 Data: Life Type: Seconds	

	Life Duration (Hex): 00015180	
	61011:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Event: EV_RCVD_MSG 61111:28:39.96508/24/12Sev=Info/5IKE/0x63000045 RESPONDER-LIFETIME notify has value of 86400 seconds 61211:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Event: EV_CHK_PFS 61311:28:39.96508/24/12Sev=Debug/7IKE/0x63000076	Process QM2.
	NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG3Event: EV_BLD_MSG 61411:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 ISAKMP Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Next Payload:Hash Ver (Hex):10 Exchange Type:Quick Mode Flags:(Encryption) MessageID(Hex):E83792E Length:52 Payload Hash Next Payload: None Reserved: 00 Payload Length: 24 Data (In Hex): CDDC20D91EB4B568C826D6A5770A5CF020141236	Construct QM3. Decrypted payload for QM3 shown here. This process ncludes hash.
	61511:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG3Event: EV_SND_MSG 61611:28:39.96508/24/12Sev=Info/4IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH) to 64.102.156.88	Send QM3. Client is now ready to encrypt and decrypt.
	<========== Quick Mode Message 3 (QM3) ==========	
Receive QM3.	Aug 24 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=e83792e) with payloads : HDR + HASH (8) + NONE (0) total length : 52	
Process QM3. Create the inbound and outbound security parameter indexes (SPIs). Add static route for the	Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, processing hash payload Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, loading all IPSEC SAs	

host.
Relevant configuration:
`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`**
	Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Generating Quick Mode Key!
	Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, NP encrypt rule look up for crypto map out-dyn-map 10 matching ACL Unknown: returned cs_id=cc107410; rule=00000000
	Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Generating Quick Mode Key!
	IPSEC: New embryonic SA created @ 0xccc9ed60,
	SCB: 0xCF7F59E0,
	Direction: outbound
	SPI: 0xC055290A
	Session ID: 0x00138000
	VPIF num: 0x00000004
	Tunnel type: ra
	Protocol: esp
	Lifetime: 240 seconds
	IPSEC: Completed host OBSA update, SPI 0xC055290A
	IPSEC: Creating outbound VPN context, SPI 0xC055290A
	Flags: 0x00000025
	SA: 0xccc9ed60
	SPI: 0xC055290A
	MTU: 1500 bytes
	VCID : 0x00000000
	Peer : 0x00000000
	SCB: 0xA5922B6B
	Channel: 0xc82afb60
	IPSEC: Completed outbound VPN context, SPI 0xC055290A
	VPN handle: 0x0015909c
	IPSEC: New outbound encrypt rule, SPI 0xC055290A
	Src addr: 0.0.0.0
	Src mask: 0.0.0.0
	Dst addr: 192.168.1.100
	Dst mask: 255.255.255.255
	Src ports
	Upper: 0
	Lower: 0
	Op: ignore
	Dst ports
	Upper: 0
	Lower: 0
	Op: ignore
	Protocol: 0
	Use protocol: false
	SPI: 0x00000000
	Use SPI: false
	IPSEC: Completed outbound encrypt rule, SPI	

	0xC055290A Rule ID: 0xcb47a710 IPSEC: New outbound permit rule, SPI 0xC055290A Src addr: 64.102.156.88 Src mask: 255.255.255.255 Dst addr: 64.102.156.87 Dst mask: 255.255.255.255 Src ports Upper: 4500 Lower: 4500 Op: equal Dst ports Upper: 58506 Lower: 58506 Op: equal Protocol: 17 Use protocol: true SPI: 0x00000000 Use SPI: false IPSEC: Completed outbound permit rule, SPI 0xC055290A Rule ID: 0xcdf3cfa0 Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, NP encrypt rule look up for crypto map out-dyn-map 10 matching ACL Unknown: returned cs_id=cc107410; rule=00000000 Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Security negotiation complete for User (user1)Responder, Inbound SPI = 0x9e18acb2, Outbound SPI = 0xc055290a Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE got a KEY_ADD msg for SA: SPI = 0xc055290a IPSEC: Completed host IBSA update, SPI 0x9E18ACB2 IPSEC: Creating inbound VPN context, SPI 0x9E18ACB2 Flags: 0x00000026 SA: 0xcfdffc90 SPI: 0x9E18ACB2 MTU: 0 bytes VCID : 0x00000000 Peer : 0x0015909C SCB: 0xA5672481 Channel: 0xc82afb60 IPSEC: Completed inbound VPN context, SPI 0x9E18ACB2 VPN handle: 0x0016219c IPSEC: Updating outbound VPN context 0x0015909C, SPI 0xC055290A Flags: 0x00000025	

SA: 0xccc9ed60
SPI: 0xC055290A
MTU: 1500 bytes
VCID : 0x00000000
Peer : 0x0016219C
SCB: 0xA5922B6B
Channel: 0xc82afb60
IPSEC: Completed outbound VPN context, SPI 0xC055290A
VPN handle: 0x0015909c
IPSEC: Completed outbound inner rule, SPI 0xC055290A
Rule ID: 0xcb47a710
IPSEC: Completed outbound outer SPD rule, SPI 0xC055290A
Rule ID: 0xcdf3cfa0
IPSEC: New inbound tunnel flow rule, SPI 0x9E18ACB2
Src addr: 192.168.1.100
Src mask: 255.255.255.255
Dst addr: 0.0.0.0
Dst mask: 0.0.0.0
Src ports
Upper: 0
Lower: 0
Op: ignore
Dst ports
Upper: 0
Lower: 0
Op: ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x9E18ACB2
Rule ID: 0xcdf15270
IPSEC: New inbound decrypt rule, SPI 0x9E18ACB2
Src addr: 64.102.156.87
Src mask: 255.255.255.255
Dst addr: 64.102.156.88
Dst mask: 255.255.255.255
Src ports
Upper: 58506
Lower: 58506
Op: equal
Dst ports
Upper: 4500
Lower: 4500
Op: equal
Protocol: 17
Use protocol: true
SPI: 0x00000000

	Use SPI: false IPSEC: Completed inbound decrypt rule, SPI 0x9E18ACB2 Rule ID: 0xce03c2f8 IPSEC: New inbound permit rule, SPI 0x9E18ACB2 Src addr: 64.102.156.87 Src mask: 255.255.255.255 Dst addr: 64.102.156.88 Dst mask: 255.255.255.255 Src ports Upper: 58506 Lower: 58506 Op: equal Dst ports Upper: 4500 Lower: 4500 Op: equal Protocol: 17 Use protocol: true SPI: 0x00000000 Use SPI: false IPSEC: Completed inbound permit rule, SPI 0x9E18ACB2 Rule ID: 0xcf6f58c0 Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Pitcher: received KEY_UPDATE, spi 0x9e18acb2 Aug 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Starting P2 rekey timer: 82080 seconds. Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Adding static route for client address: 192.168.1.100	
Phase 2 complete. Both sides are encrypting and decrypting now.	Aug 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, PHASE 2 COMPLETED (msgid=0e83792e)	
For hardware clients, one more message is received where the client sends information about itself. If you look carefully, you should find the hostname of EzVPN client, software that is run on the client, and location and name of the software	Aug 24 11:31:13 [IKEv1]: IP = 10.48.66.23, IKE_DECODE RECEIVED Message (msgid=91facca9) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 184 Aug 24 11:31:13 [IKEv1 DEBUG]: Group = EZ, Username = cisco, IP = 10.48.66.23, processing hash payload Aug 24 11:31:13 [IKEv1 DEBUG]: Group = EZ, Username = cisco, IP = 10.48.66.23, processing notify payload Aug 24 11:31:13 [IKEv1 DECODE]: OBSOLETE DESCRIPTOR - INDEX 1 Aug 24 11:31:13 [IKEv1 DECODE]: 0000: 00000000 7534000B 62736E73 2D383731 ....u4..**bsns-871**	

	0010: 2D332E75 32000943 6973636F 20383731 **-3**.u2..**Cisco 871** 0020: 7535000B 46484B30 39343431 32513675 u5..FHK094412Q6u 0030: 36000932 32383538 39353638 75390009 6..228589568u9.. 0040: 31343532 31363331 32753300 2B666C61 145216312u3.+**fla** 0050: 73683A63 3837302D 61647669 70736572 **sh:c870-advipser** 0060: 76696365 736B392D 6D7A2E31 32342D32 **vicesk9-mz.124-2** 0070: 302E5435 2E62696E **0.T5.bin** Aug 24 11:31:13 [IKEv1 DEBUG]: Group = EZ, Username = cisco, IP = 10.48.66.23, Processing PSK Hash Aug 24 11:31:13 [IKEv1]: Group = EZ, Username = cisco, IP = 192.168.1.100, Inconsistent PSK hash size Aug 24 11:31:13 [IKEv1 DEBUG]: Group = EZ, Username = cisco, IP = 10.48.66.23, PSK Hash Verification Failed!	

Tunnel Verification

ISAKMP

Output from the **sh cry isa sa det** command is:

```
 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: 10.48.66.23
 Type : user Role : responder
 Rekey : no State : AM_ACTIVE
 Encrypt : aes Hash : SHA
 Auth : preshared Lifetime: 86400
 Lifetime Remaining: 86387
 AM_ACTIVE - aggressive mode is active.
```

IPsec

Since the Internet Control Message Protocol (ICMP) is used to trigger the tunnel, only one IPsec SA is up. Protocol 1 is ICMP. Note that the SPI values differ from the ones negotiated in the debugs. This is, in fact, the same tunnel after the Phase 2 rekey.

Output from the **sh crypto ipsec sa** command is:

```
interface: outside
 Crypto map tag: DYN, seq num: 10, local addr: 10.48.67.14
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.100/255.255.255.255/0/0)
current_peer: 10.48.66.23, username: cisco
dynamic allocated peer ip: 192.168.1.100

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 5, #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.: 10.48.67.14/0, remote crypto endpt.: 10.48.66.23/0
path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: C4B9A77C
current inbound spi : EA2B6B15

inbound esp sas:
spi: 0xEA2B6B15 (3928714005)
transform: esp-aes esp-sha-hmac no compression
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 425984, crypto-map: DYN
sa timing: remaining key lifetime (sec): 28714
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000003F
outbound esp sas:
spi: 0xC4B9A77C (3300501372)
transform: esp-aes esp-sha-hmac no compression
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 425984, crypto-map: DYN
sa timing: remaining key lifetime (sec): 28714
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

Related Information

- **Wikipedia Article on IPsec**
- **IPsec Troubleshooting: Understanding and Using debug Commands**
- **Technical Support & Documentation - Cisco Systems**