ASA IKEv2 Debugs for Remote Access VPN Troubleshooting

Document ID: 116158

Contributed by Anu M. Chacko, Jay Young, and Atri Basu, Cisco TAC Engineers.
Oct 09, 2013

Contents

Introduction

This document describes how to understand debugs on the Cisco Adaptive Security Appliance (ASA) when Internet Key Exchange Version 2 (IKEv2) is used with a Cisco AnyConnect Secure Mobility Client. This document also provides information on how to translate certain debug lines in an ASA configuration.

This document does not describe how to pass traffic after a VPN tunnel has been established to the ASA, nor does it include basic concepts of IPSec or IKE.

Prerequisites

Requirements

Cisco recommends that you have knowledge of the packet exchange for IKEv2. For more information, refer to IKEv2 Packet Exchange and Protocol Level Debugging.

Components Used

The information in this document is based on these software and hardware versions:

- Internet Key Exchange Version 2 (IKEv2)
- Cisco Adaptive Security Appliance (ASA) Version 8.4 or later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Core Issue

The Cisco Technical Assistance Center (TAC) often uses IKE and IPSec debug commands in order to understand where there is a problem with IPSec VPN tunnel establishment, but the commands can be cryptic.

Scenario

Debug Commands

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
debug aggregate-auth xml 5
```

ASA Configuration

This ASA configuration is strictly basic, with no use of external servers.

```
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.0.0.1 255.255.255.0

ip local pool webvpn1 10.2.2.1-10.2.2.10

crypto ipsec ikev2 ipsec-proposal 3des
 protocol esp encryption aes-256 aes 3des des
 protocol esp integrity sha-1
crypto dynamic-map dynmap 1000 set ikev2 ipsec-proposal 3des
crypto map crymap 10000 ipsec-isakmp dynamic dynmap
crypto map crymap interface outside

crypto ca trustpoint Anu-ikev2
 enrollment self
 crl configure

crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 2
 prf sha
 lifetime seconds 86400

crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint Anu-ikev2
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1
ssl trust-point Anu-ikev2 outside

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.0.1047-k9.pkg 1
 anyconnect profiles Anyconnect-ikev2 disk0:/anyconnect-ikev2.xml
 anyconnect enable
 tunnel-group-list enable

group-policy ASA-IKEV2 internal
group-policy ASA-IKEV2 attributes
```

```
 wins-server none
 dns-server none
 vpn-tunnel-protocol ikev2
 default-domain none
 webvpn
  anyconnect modules value dart
  anyconnect profiles value Anyconnect-ikev2 type user

username Anu password lAuoFgF7KmB3D0WI encrypted privilege 15

tunnel-group ASA-IKEV2 type remote-access
tunnel-group ASA-IKEV2 general-attributes
 address-pool webvpn1
 default-group-policy ASA-IKEV2
tunnel-group ASA-IKEV2 webvpn-attributes
 group-alias ASA-IKEV2 enable
```

XML File

```
<ServerList>
        <HostEntry>
                <HostName>Anu-IKEV2</HostName>
                <HostAddress>10.0.0.1</HostAddress>
                <UserGroup>ASA-IKEV2</UserGroup>
                <PrimaryProtocol>IPsec</PrimaryProtocol>
        </HostEntry>
</ServerList>
```

Note: The UserGroup name in the XML client profile must be the same as the name of the tunnel−group on the ASA. Otherwise, the error message 'Invalid Host Entry. Please re−enter' is seen on the AnyConnect client.

Debug Logs and Descriptions

Note: Logs from the Diagnostics and Reporting Tool (DART) are generally very chatty, so certain DART logs have been omitted in this example due to insignificance.

Server Message Description ***Debugs***

Date : 04/23/2013
Time : 16:24:55
Type : Information
Source : acvpnui

Description : Function: ClientIfcBase::connect
File: .\ClientIfcBase.cpp
Line: 964
A VPN connection to Anu−IKEV2 has been requested by the user.

****
Date : 04/23/2013
Time : 16:24:55
Type : Information
Source : acvpnui

Description : Message type information sent to the user:
Contacting Anu−IKEV2.
****

Date : 04/23/2013
Time : 16:24:55
Type : Information
Source : acvpnui

Description : Function: ApiCert::getCertList
File: .\ApiCert.cpp
Line: 259
Number of certificates found: 0
****
Date : 04/23/2013
Time : 16:25:00
Type : Information
Source : acvpnui

Description : ***Initiating VPN connection to the secure gateway https://10.0.0.1***
****
Date : 04/23/2013
Time : 16:25:00
Type : Information
Source : acvpnagent

Description : Tunnel initiated by GUI Client.

****

Date : 04/23/2013
Time : 16:25:02
Type : Information
Source : acvpnagent

Description : Function: CIPsecProtocol::connectTransport
File: .\IPsecProtocol.cpp
Line: 1629
Opened IKE socket from 192.168.1.1:25170 to 10.0.0.1:500
****
----------IKE_SA_INIT Exchange starts----------

The ASA receives the IKE_SA_INIT message from the client.

IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT] [192.168.1.1]:25170->[10.0.0.1
InitSPI=0x58aff71141ba436b RespSPI=0x0000000000000000 MID=00000000

IKEv2-PROTO-3: Rx [L 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0] m_id:

The first pair of messages is the IKE_SA_INIT exchange. These messages negotiate cryptographic algorithms, exchange nonces, and do a Diffie-Hellman (DH) exchange.

IKEv2-PROTO-3: ***HDR***[i:58AFF71141BA436B - r: 0000000000000000]
IKEv2-PROTO-4: IKEV2 HDR ***ispi: 58AFF71141BA436B - rspi: 00000000***
IKEv2-PROTO-4: Next payload: SA, ***version: 2.0***
IKEv2-PROTO-4: Exchange type: IKE_SA_INIT, ***flags: INITIATOR***
IKEv2-PROTO-4: Message id: 0x0, length: 528

The IKE_SA_INIT message received from the client contains these fields:

1. ***ISAKMP Header*** - SPI/version/flags.

SA Next payload: KE, reserved: 0x0, length: 168
IKEv2-PROTO-4: last proposal: 0x0, reserved: 0x0, length: 164
Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 18
IKEv2-PROTO-4: last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC

2. ***SAi1*** − Cryptographic algorithm that IKE initiator supports.
3. ***KEi*** − DH public key value of the initiator.
4. ***N*** − Initiator Nonce.

IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES−CBC
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES−CBC
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 1, reserved: 0x0, id: 3DES
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 1, reserved: 0x0, id: DES
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA512
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA384
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA256
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA1
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: MD5
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA512
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA384
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA256
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: MD596
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1536_MODP/Group 5
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2
IKEv2−PROTO−4: last transform: 0x0, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_768_MODP/Group 1

KE Next payload: N, reserved: 0x0, length: 104
DH group: 1, Reserved: 0x0

eb 5e 29 fe cb 2e d1 28 ed 4a 54 b1 13 7c b8 89
f7 62 13 6b df 95 88 28 b5 97 ba 52 ef e4 1d 28
ca 06 d1 36 b6 67 32 9a c2 dd 4e d8 c7 80 de 20
36 34 c5 b3 3e 1d 83 1a c7 fb 9d b8 c5 f5 ed 5f
ba ba 4f b6 b2 e2 2d 43 4f a0 b6 90 9a 11 3f 7d
0a 21 c3 4d d3 0a d2 1e 33 43 d3 5e cc 4b 38 e0

N Next payload: VID, reserved: 0x0, length: 24

20 12 8f 22 7b 16 23 52 e4 29 4d 98 c7 fd a8 77
ce 7c 0b b4

IKEv2−PROTO−5: Parse Vendor Specific Payload: CISCO−DELETE−REASC
payload: VID, reserved: 0x0, length: 23

The ASA verifies and processes the IKE_INIT message. The ASA:

Decrypted packet:Data: 528 bytes
IKEv2−PLAT−3: Process custom VID payloads
IKEv2−PLAT−3: Cisco Copyright VID received from peer
IKEv2−PLAT−3: AnyConnect EAP VID received from peer

1. Chooses the crypto suite from
those offered by the initiator.
2. Computes its own DH secret key.
3. Computes a SKEYID value from
which all keys can be derived for
this IKE_SA. The headers of all
subsequent messages are
encrypted and authenticated. The
keys used for the encryption and
integrity protection are derived
from SKEYID and are known as:
    1. ***SK_e*** − Encryption.
    2. ***SK_a*** − Authentication.
    3. ***SK_d*** − Derived and used
    for derivation of further
    keying material for CHILD_SAs.

A separate SK_e and SK_a are
computed for each direction.

Relevant Configuration:

```
crypto ikev2 policy 10
 encryption aes-192 integrity
 sha group 2  prf sha lifetime
 seconds 86400
crypto ikev2 enable outside
```

IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: IDLE Event: ***E***
IKEv2−PROTO−3: (6): Check NAT discovery
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: IDLE Event: EV_CHK_REDIRECT
IKEv2−PROTO−5: (6): Redirect check is not needed, skipping it
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: IDLE Event: E
IKEv2−PLAT−5: ***New ikev2 sa request admitted***
IKEv2−PLAT−5: Incrementing incoming negotiating sa count by one
IKEv2−PLAT−5: INVALID PSH HANDLE
IKEv2−PLAT−5: INVALID PSH HANDLE
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: IDLE Event: EV_CHK_COOKIE
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: IDLE Event: EV_CHK4_COOKIE_NOTIFY
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_INIT Event: ***EV_VERIFY_MSG***
IKEv2−PROTO−3: (6): ***Verify SA init message***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_INIT Event: EV_INSERT_SA
IKEv2−PROTO−3: (6): Insert SA
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_INIT Event: EV_GET_IKE_POLICY
IKEv2−PROTO−3: (6): ***Getting configured policies***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_INIT Event: ***EV_PROC_MSG***
IKEv2−PROTO−2: (6): Processing initial message
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_INIT Event: EV_DETECT_NAT
IKEv2−PROTO−3: (6): Process NAT discovery notify
IKEv2−PROTO−5: (6): Processing nat detect src notify
IKEv2−PROTO−5: (6): Remote address not matched
IKEv2−PROTO−5: (6): Processing nat detect dst notify
IKEv2−PROTO−5: (6): Local address matched
IKEv2−PROTO−5: (6): Host is located NAT outside
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_INIT Event: EV_CHK_CONFIG_MODE
IKEv2−PROTO−3: (6): Received valid config mode data
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_INIT Event: EV_SET_RECD_CONFIG_MODE
IKEv2−PROTO−3: (6): Set received config mode data
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_BLD_INIT

EV_SET_POLICY
IKEv2−PROTO−3: (6): ***Setting configured policies***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_BLD_INIT
EV_CHK_AUTH4PKI
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_BLD_INIT
EV_PKI_SESH_OPEN
IKEv2−PROTO−3: (6): Opening a PKI session
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_BLD_INIT
EV_GEN_DH_KEY
IKEv2−PROTO−3: (6): ***Computing DH public key***
IKEv2−PROTO−3: (6):
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_BLD_INIT
EV_NO_EVENT
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_BLD_INIT
EV_OK_RECD_DH_PUBKEY_RESP
IKEv2−PROTO−5: (6): Action: Action_Null
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_BLD_INIT
EV_GEN_DH_SECRET
IKEv2−PROTO−3: (6): ***Computing DH secret key***
IKEv2−PROTO−3: (6):
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_BLD_INIT
EV_NO_EVENT
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_BLD_INIT
EV_OK_RECD_DH_SECRET_RESP
IKEv2−PROTO−5: (6): Action: Action_Null
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_BLD_INIT
EV_GEN_SKEYID
IKEv2−PROTO−3: (6): ***Generate skeyid***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_BLD_INIT
EV_GET_CONFIG_MODE

The ASA constructs the response message for IKE_SA_INIT exchange.

This packet contains:

1. ***ISAKMP Header*** − SPI/version/flags.
2. ***SAr1*** − Cryptographic algorithm that IKE responder chooses.
3. ***KEr*** − DH public key value of the responder.
4. ***N*** − Responder Nonce.

IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_BLD_INIT
EV_BLD_MSG
IKEv2−PROTO−2: (6): ***Sending initial message***
IKEv2−PROTO−3: IKE Proposal: 1, SPI size: 0 (initial negotiation),
Num. transforms: 4
AES−CBC SHA1 SHA96 DH_GROUP_768_MODP/Group 1
IKEv2−PROTO−5: Construct Vendor Specific Payload: DELETE−REASONIK
Construct Vendor Specific Payload: (CUSTOM)IKEv2−PROTO−5: Construct
Payload: (CUSTOM)IKEv2−PROTO−5: Construct Notify Payload:
NAT_DETECTION_SOURCE_IPIKEv2−PROTO−5: Construct Notify Payloa
NAT_DETECTION_DESTINATION_IPIKEv2−PLAT−2: Failed to retrieve tru
hashes or none available
IKEv2−PROTO−5: Construct Vendor Specific Payload:

FRAGMENTATIONIKEv2−PROTO−3: Tx [L 10.0.0.1:500/R 192.168.1.1:251
m_id: 0x0
IKEv2−PROTO−3: ***HDR***[i:58AFF71141BA436B − r: FC696330E6B94D7F]
IKEv2−PROTO−4: IKEV2 HDR ***ispi: 58AFF71141BA436B − rspi: FC69633***
IKEv2−PROTO−4: Next payload: SA, version: 2.0
IKEv2−PROTO−4: Exchange type: IKE_SA_INIT, ***flags: RESPONDER MSG***
IKEv2−PROTO−4: Message id: 0x0, length: 386
SA Next payload: KE, reserved: 0x0, length: 48
IKEv2−PROTO−4: last proposal: 0x0, reserved: 0x0, length: 44
Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES−CBC
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA1
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
IKEv2−PROTO−4: last transform: 0x0, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_768_MODP/Group 1

KE Next payload: N, reserved: 0x0, length: 104
DH group: 1, Reserved: 0x0

c9 30 f9 32 d4 7c d1 a7 5b 71 72 09 6e 7e 91 0c
e1 ce b4 a4 3c f2 8b 74 4e 20 59 b4 0b a1 ff 65
37 88 cc c4 a4 b6 fa 4a 63 03 93 89 e1 7e bd 6a
64 9a 38 24 e2 a8 40 f5 a3 d6 ef f7 1a df 33 cc
a1 8e fa dc 9c 34 45 79 1a 7c 29 05 87 8a ac 02
98 2e 7d cb 41 51 d6 fe fc c7 76 83 1d 03 b0 d7
N Next payload: VID, reserved: 0x0, length: 24

c2 28 7f 8c 7d b3 1e 51 fc eb f1 97 ec 97 b8 67
d5 e7 c2 f5
VID Next payload: VID, reserved: 0x0, length: 23

The ASA sends out the response message for IKE_SA_INIT exchange. The IKE_SA_INIT exchange is now complete. The ASA starts the timer for the authentication process.

IKEv2−PLAT−4: SENT PKT [IKE_SA_INIT] [10.0.0.1]:500−>[192.168.1.1]:25170 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000000
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: INIT_DONE Event: EV_DONE
IKEv2−PROTO−3: (6): Fragmentation is enabled
IKEv2−PROTO−3: (6): Cisco DeleteReason Notify is enabled
IKEv2−PROTO−3: (6): Complete SA init exchange
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: INIT_DONE Event:

****
Date : 04/23/2013
Time : 16:25:02
Type : Information
Source : acvpnagent

Description : Function: CIPsecProtocol::initiateTunnel
File: .\IPsecProtocol.cpp
Line: 345
IPsec tunnel is initiating
****

EV_CHK4_ROLE
IKEv2−PROTO−5: (6): SM Trace−> SA:
I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID =
00000000 CurState: INIT_DONE Event:
EV_START_TMR
IKEv2−PROTO−3: (6): Starting timer to wait
for auth message (30 sec)
IKEv2−PROTO−5: (6): SM Trace−> SA:
I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID =
00000000 CurState: R_WAIT_AUTH Event:
EV_NO_EVENT

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−IKE_SA_INIT Complete−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

−−− IKE_AUTH Begins−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

****
Date : 04/23/2013
Time : 16:25:00
Type : Information
Source : acvpnagent

Description : Secure Gateway Parameters:
IP Address: 10.0.0.1
Port: 443
URL: "10.0.0.1"
Auth method: ***IKE − EAP−AnyConnect***
IKE Identity:
****
Date : 04/23/2013
Time : 16:25:00
Type : Information
Source : acvpnagent

Description : ***Initiating Cisco AnyConnect Secure Mobility Client connection,***
****

Date : 04/23/2013
Time : 16:25:02
Type : Information
Source : acvpnagent

Description : Function: ikev2_log
File: .\ikev2_anyconnect_osal.cpp
Line: 2730
Received request to establish an IPsec tunnel; local traffic selector = Address 0.0.0.0−255.255.255.255 Protocol: 0 Port Range: 0−65535 ; remote traffic sel Range: 0.0.0.0−255.255.255.255 Protocol: 0 Port Range: 0−65535
****
Date : 04/23/2013
Time : 16:25:02

Type : Information
Source : acvpnagent

Description : Function: CIPsecProtocol::connectTransport
File: .\IPsecProtocol.cpp
Line: 1629
Opened IKE socket from 192.168.1.1:25171 to 10.0.0.1:4500
****

Authentication is done with EAP. Only a single EAP authentication method is allowed within an EAP conversation. The ASA receives the IKE_AUTH message from the client.

IKEv2−PLAT−4: ***RECV PKT [IKE_AUTH]*** [192.168.1.1]:25171−>[10.0.0.1]:4
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000001

IKEv2−PROTO−3: ***Rx*** [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id

When the client includes an IDi payload
but not an AUTH payload, this indicates
the client has declared an identity but has
not proven it. In the debugs, the AUTH
payload is not present in the IKE_AUTH
packet sent by the client. The client sends the AUTH payload only after the
EAP exchange is successful. If the ASA
is willing to use an extensible authentication method, it places an EAP
payload in message 4 and defers sending
SAr2, TSi, and TSr until the initiator authentication is complete in a subsequent IKE_AUTH exchange.

IKEv2−PROTO−3: ***HDR***[i:58AFF71141BA436B − r: FC696330E6B94D7F]
IKEv2−PROTO−4: IKEV2 ***HDR ispi: 58AFF71141BA436B − rspi: FC69633***
IKEv2−PROTO−4: Next payload: ENCR, ***version: 2.0***
IKEv2−PROTO−4: Exchange type: IKE_AUTH, ***flags: INITIATOR***
IKEv2−PROTO−4: Message id: 0x1, length: 540
IKEv2−PROTO−5: (6): Request has mess_id 1; expected 1 through 1
REAL Decrypted packet:Data: 465 bytes
IKEv2−PROTO−5: Parse Vendor Specific Payload: (CUSTOM) VID Next pay
reserved: 0x0, length: 20

58 af f6 11 52 8d b0 2c b8 da 30 46 be 91 56 fa
IDi Next payload: CERTREQ, reserved: 0x0, length: 28
Id type: Group name, Reserved: 0x0 0x0

2a 24 41 6e 79 43 6f 6e 6e 65 63 74 43 6c 69 65
6e 74 24 2a
CERTREQ Next payload: CFG, reserved: 0x0, length: 25
Cert encoding X.509 Certificate − signature
CertReq data: 20 bytes
CFG Next payload: SA, reserved: 0x0, length: 196
cfg type: ***CFG_REQUEST***, reserved: 0x0, reserved: 0x0

attrib type: internal IP4 address, length: 0

attrib type: internal IP4 netmask, length: 0

attrib type: internal IP4 DNS, length: 0

attrib type: internal IP4 NBNS, length: 0

attrib type: internal address expiry, length: 0

attrib type: application version, length: 27

41 6e 79 43 6f 6e 6e 65 63 74 20 57 69 6e 64 6f
77 73 20 33 2e 30 2e 31 30 34 37
attrib type: internal IP6 address, length: 0

attrib type: internal IP4 subnet, length: 0

The IKE_AUTH initiator packet contains:

1. ***ISAKMP Header*** − SPI/version/flags.
2. ***IDi*** − The tunnel−group name that the client wishes to connect to may be delivered by the IDi payload of type ID_KEY_ID in the initial message of the IKE_AUTH exchange. This occurs when the client profile* is

preconfigured with a group name
or, after a previous successful authentication, the client has cached the group name in its preferences file. The ASA attempts to match a tunnel−group name with the contents of the IKE IDi payload. After the first successful IPSec VPN is established, the client caches the group name (group alias) to which the user authenticated. This group name is delivered in the IDi payload of the next connection attempt in order to indicate the probable group desired by the user. When EAP authentication is specified or implied by the client profile and the profile does not contain the <IKEIdentity> element, the client sends an ID_GROUP type IDi payload with the fixed string *$AnyConnectClient$*.

3. ***CERTREQ*** − The client is requesting the ASA for a preferred certificate. Certificate request payloads may be included in an exchange when the sender needs to get the certificate of the receiver. The certificate request payload is processed by inspection of the 'Cert encoding' field in order to determine whether the processor has any certificates of this type. If so,

attrib type: Unknown − 28682, length: 15
77 69 6e 78 70 36 34 74 65 6d 70 6c 61 74 65
attrib type: Unknown − 28704, length: 0
attrib type: Unknown − 28705, length: 0
attrib type: Unknown − 28706, length: 0
attrib type: Unknown − 28707, length: 0
attrib type: Unknown − 28708, length: 0
attrib type: Unknown − 28709, length: 0
attrib type: Unknown − 28710, length: 0
attrib type: Unknown − 28672, length: 0
attrib type: Unknown − 28684, length: 0
attrib type: Unknown − 28711, length: 2
05 7e
attrib type: Unknown − 28674, length: 0
attrib type: Unknown − 28712, length: 0
attrib type: Unknown − 28675, length: 0
attrib type: Unknown − 28679, length: 0
attrib type: Unknown − 28683, length: 0
attrib type: Unknown − 28717, length: 0
attrib type: Unknown − 28718, length: 0
attrib type: Unknown − 28719, length: 0
attrib type: Unknown − 28720, length: 0
attrib type: Unknown − 28721, length: 0
attrib type: Unknown − 28722, length: 0
attrib type: Unknown − 28723, length: 0
attrib type: Unknown − 28724, length: 0
attrib type: Unknown − 28725, length: 0
attrib type: Unknown − 28726, length: 0

the 'Certification Authority' field is inspected in order to determine if the processor has any certificates that can be validated up to one of the specified certification authorities. This can be a chain of certificates.

4. ***CFG*** − CFG_REQUEST/ CFG_REPLY allows an IKE endpoint to request information from its peer. If an attribute in the CFG_REQUEST configuration payload is not zero−length, it is taken as a suggestion for that attribute.The CFG_REPLY configuration payload may return that value or a new one. It may also add new attributes and not include some requested ones. Requestors ignore returned attributes that they do not recognize. In these debugs, the client is requesting the tunnel configuration in the CFG_REQUEST. The ASA replies to this and sends the tunnel configuration attributes only after the EAP exchange is successful.
5. ***SAi2*** − SAi2 initiates the SA, which is similar to the phase 2 transform set exchange in IKEv1.
6. ***TSi*** and ***TSr*** − The initiator and responder traffic selectors contain, respectively, the

```
        attrib type: Unknown − 28727, length: 0

        attrib type: Unknown − 28729, length: 0

SA      Next payload: TSi, reserved: 0x0, length: 124
IKEv2−PROTO−4:   last proposal: 0x0, reserved: 0x0, length: 120
  Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 12
IKEv2−PROTO−4:     last transform: 0x3, reserved: 0x0: length: 12
    type: 1, reserved: 0x0, id: AES−CBC
IKEv2−PROTO−4:     last transform: 0x3, reserved: 0x0: length: 12
    type: 1, reserved: 0x0, id: AES−CBC
IKEv2−PROTO−4:     last transform: 0x3, reserved: 0x0: length: 12
    type: 1, reserved: 0x0, id: AES−CBC
IKEv2−PROTO−4:     last transform: 0x3, reserved: 0x0: length: 8
    type: 1, reserved: 0x0, id: 3DES
IKEv2−PROTO−4:     last transform: 0x3, reserved: 0x0: length: 8
    type: 1, reserved: 0x0, id: DES
IKEv2−PROTO−4:     last transform: 0x3, reserved: 0x0: length: 8
    type: 1, reserved: 0x0, id: NULL
IKEv2−PROTO−4:     last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: SHA512
IKEv2−PROTO−4:     last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: SHA384
IKEv2−PROTO−4:     last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: SHA256
IKEv2−PROTO−4:     last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: SHA96
IKEv2−PROTO−4:     last transform: 0x3, reserved: 0x0: length: 8
    type: 3, reserved: 0x0, id: MD596
IKEv2−PROTO−4:     last transform: 0x0, reserved: 0x0: length: 8
    type: 5, reserved: 0x0, id:

TSi     Next payload: TSr, reserved: 0x0, length: 24
  Num of TSs: 1, reserved 0x0, reserved 0x0
  TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
  start port: 0, end port: 65535
  start addr: 0.0.0.0, end addr: 255.255.255.255
TSr     Next payload: NOTIFY, reserved: 0x0, length: 24
  Num of TSs: 1, reserved 0x0, reserved 0x0
  TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
  start port: 0, end port: 65535
  start addr: 0.0.0.0, end addr: 255.255.255.255
```

source
and destination address of the
initiator and responder in
order to
forward and receive
encrypted
traffic. The address range
specifies that all traffic to and
from
that range is tunneled. If the
proposal is acceptable to the
responder, it sends identical
TS
payloads back.

The attributes the client must deliver
for
group authentication are stored in an
AnyConnect profile file.

Relevant Profile Configuration:

```
<ServerList>
<HostEntry>
  <HostName>Anu−IKEV2
  </HostName>
  <HostAddress>10.0.0.1
  </HostAddress>
  <UserGroup>ASA−IKEV2
  </UserGroup>
<PrimaryProtocol>IPsec
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

The ASA generates a response to the IKE_AUTH message and prepares to authenticate itself to the client.

Decrypted packet:Data: 540 bytes
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_WAIT_AUT
EV_RECV_AUTH
IKEv2−PROTO−3: (6): Stopping timer to wait for auth message
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_WAIT_AUT
EV_CHK_NAT_T
IKEv2−PROTO−3: (6): Check NAT discovery
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_WAIT_AUT
EV_CHG_NAT_T_PORT
IKEv2−PROTO−2: (6): NAT detected float to init port 25171, resp port 4500
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_WAIT_AUT
EV_PROC_ID
IKEv2−PROTO−2: (6): Recieved valid parameteres in process id
IKEv2−PLAT−3: (6) peer auth method set to: 0
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_WAIT_AUT
EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_WAIT_AUT
EV_GET_POLICY_BY_PEERID
IKEv2−PROTO−3: (6): Getting configured policies
IKEv2−PLAT−3: New AnyConnect Client connection detected based on ID pay
IKEv2−PLAT−3: my_auth_method = 1
IKEv2−PLAT−3: (6) peer auth method set to: 256
IKEv2−PLAT−3: supported_peers_auth_method = 16
IKEv2−PLAT−3: (6) tp_name set to: Anu−ikev2
IKEv2−PLAT−3: ***trust point set to:*** Anu−ikev2
IKEv2−PLAT−3: P1 ID = 0
IKEv2−PLAT−3: Translating IKE_ID_AUTO to = 9
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_WAIT_AUT
EV_SET_POLICY
IKEv2−PROTO−3: (6): ***Setting configured policies***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_WAIT_AUT
EV_VERIFY_POLICY_BY_PEERID
IKEv2−PROTO−3: (6): Verify peer's policy
IKEv2−PROTO−3: (6): ***Matching certificate found***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_WAIT_AUT
EV_CHK_CONFIG_MODE
IKEv2−PROTO−3: (6): Received valid config mode data
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_WAIT_AUT
EV_SET_RECD_CONFIG_MODE
IKEv2−PLAT−3: (6) DHCP hostname for DDNS is set to: winxp64template
IKEv2−PROTO−3: (6): Set received config mode data
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_WAIT_AUT
EV_CHK_AUTH4EAP
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_WAIT_AUT
EV_CHK_EAP
IKEv2−PROTO−3: (6): ***Check for EAP exchange***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: ***R_BLD_AUTH***
EV_GEN_AUTH
IKEv2−PROTO−3: (6): ***Generate my authentication data***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_BLD_AUTH
EV_CHK4_SIGN
IKEv2−PROTO−3: (6): Get my authentication method
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_BLD_AUTH
EV_SIGN
IKEv2−PROTO−3: (6): ***Sign auth data***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_BLD_AUTH
EV_OK_AUTH_GEN
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_BLD_EAP_
Event: EV_AUTHEN_REQ

IKEv2−PROTO−2: (6): ***Asking the authenticator to send EAP request***

Created element name ***config−auth value***
Added attribute name client value vpn to element config−auth
Added attribute name type value hello to element config−auth
Created element name version value 9.0(2)8
Added element name version value 9.0(2)8 to element config−auth
Added attribute name who value sg to element version
Generated XML message below
<?xml version="1.0" encoding="UTF−8"?>
<config−auth client="vpn" ***type="hello***">
<version who="sg">9.0(2)8</version>
</config−auth>

IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_BLD_EAP_
Event: EV_RECV_EAP_AUTH
IKEv2−PROTO−5: (6): Action: Action_Null
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_BLD_EAP_
Event: EV_CHK_REDIRECT
IKEv2−PROTO−3: (6): Redirect check with platform for load−balancing
IKEv2−PLAT−3: Redirect check on platform
IKEv2−PLAT−3: ikev2_osal_redirect: Session accepted by 10.0.0.1
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: R_BLD_EAP_
Event: EV_SEND_EAP_AUTH_REQ
IKEv2−PROTO−2: (6): ***Sending EAP request***
IKEv2−PROTO−5: Construct Vendor Specific Payload: CISCO−GRANITEIKE
(6): Build

The ASA sends the AUTH payload in order to request user credentials from the client. The ASA sends the AUTH method as 'RSA,' so it sends its own certificate to the client, so the client can authenticate the ASA server.

IDr Next payload: CERT, reserved: 0x0, length: 36
Id type: DER ASN1 DN, Reserved: 0x0 0x0

30 1a 31 18 30 16 06 09 2a 86 48 86 f7 0d 01 09
02 16 09 41 53 41 2d 49 4b 45 56 32
CERT Next payload: CERT, reserved: 0x0, length: 436
Cert encoding X.509 Certificate − signature
Cert data: 431 bytes
CERT Next payload: AUTH, reserved: 0x0, length: 436
Cert encoding X.509 Certificate − signature
Cert data: 431 bytes

Since the ASA is willing to use an extensible authentication method, it places an EAP payload in message 4 and defers sending SAr2, TSi, and TSr until the initiator authentication is complete in a subsequent IKE_AUTH exchange. Thus, those three payloads are not present in the debugs.

AUTH Next payload: EAP, reserved: 0x0, length: 136
Auth method RSA, reserved: 0x0, reserved 0x0
Auth data: 128 bytes
EAP Next payload: NONE, reserved: 0x0, length: 154
Code: request: ***id***: 1, ***length***: 150
Type: Unknown − 254
EAP data: 145 bytes

The EAP packet contains:

1. ***Code: request*** − This code is sent by the authenticator to the peer.

IKEv2−PROTO−3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id
IKEv2−PROTO−3: ***HDR***[i:58AFF71141BA436B − r: FC696330E6B94D7F]
IKEv2−PROTO−4: ***IKEV2 HDR ispi: 58AFF71141BA436B − rspi: FC69633***
IKEv2−PROTO−4: Next payload: ENCR, version: 2.0
IKEv2−PROTO−4: Exchange type: IKE_AUTH, ***flags: RESPONDER MSG−R***

2. ***id: 1*** − The id helps match the EAP responses with the requests. Here the value is 1, which indicates it is the first packet in the EAP exchange. This EAP request has the 'config−auth' type of 'hello;' it is sent from the ASA to the client in order to initiate the EAP exchange.
3. ***Length: 150*** − Length of the EAP packet includes the code, id, length, and EAP data.
4. ***EAP data***.

IKEv2−PROTO−4: Message id: 0x1, length: 1292
ENCR Next payload: VID, reserved: 0x0, length: 1264
Encrypted data: 1260 bytes

Fragmentation can result if the certificates are large or if certificate chains are included. Both initiator and responder KE payloads can also include large keys, which can also contribute to fragmentation.

IKEv2−PROTO−5: (6): Fragmenting packet, Fragment MTU: 544, ***Number of***
Fragment ID: 1
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000001
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000001
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000001

****

Date : 04/23/2013
Time : 16:25:02
Type : Information
Source : acvpnagent

Description : Function: ikev2_verify_X509_SIG_certs
File: .\ikev2_anyconnect_osal.cpp
Line: 2077
Requesting certificate acceptance from user

****

Date : 04/23/2013
Time : 16:25:02
Type : Error
Source : acvpnui

Description : Function: CCapiCertificate::verifyChainPolicy
File: .\Certificates\CapiCertificate.cpp
Line: 2032
Invoked Function: CertVerifyCertificateChainPolicy
Return Code: −2146762487 (0x800B0109)
Description: A certificate chain processed, but terminated in a root certificate w
by the trust provider.

****

Date : 04/23/2013
Time : 16:25:04
Type : Information
Source : acvpnagent

Description : Function: CEAPMgr::dataRequestCB

File: .\EAPMgr.cpp
Line: 400
EAP proposed type: EAP−ANYCONNECT
****

The client responds to the EAP request with a response.

The EAP packet contains:

1. ***Code: response*** − This code is sent by the peer to the authenticator in response to the EAP request.
2. ***id: 1*** − The id helps match the EAP responses with the requests. Here the value is 1, which indicates that this is a response to the request previously sent by the ASA (authenticator). This EAP response has the 'config−auth' type of 'init'; the client is initializing the EAP exchange and is waiting for the ASA to generate the authentication request.
3. ***Length: 252*** − Length of the EAP packet includes the code, id, length, and EAP data.
4. ***EAP data***.

IKEv2−PLAT−4: ***RECV PKT [IKE_AUTH]*** [192.168.1.1]:25171−>[10.0.0.1]:4
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000002
IKEv2−PROTO−3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id
IKEv2−PROTO−3: HDR[i:58AFF71141BA436B − r: FC696330E6B94D7F]
IKEv2−PROTO−4: IKEV2 HDR ispi: 58AFF71141BA436B − rspi: FC696330
IKEv2−PROTO−4: Next payload: ENCR, version: 2.0
IKEv2−PROTO−4: Exchange type: IKE_AUTH, flags: INITIATOR
IKEv2−PROTO−4: Message id: 0x2, length: 332
IKEv2−PROTO−5: (6): Request has mess_id 2; expected 2 through 2
REAL Decrypted packet:Data: 256 bytes
EAP Next payload: NONE, reserved: 0x0, length: 256
Code: response: ***id: 1***, ***length***: 252
Type: Unknown − 254
EAP data:247 bytes

Decrypted packet:Data: 332 bytes
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: R_WAIT_EAP
EV_RECV_AUTH
IKEv2−PROTO−3: (6): Stopping timer to wait for auth message
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: R_WAIT_EAP
EV_RECV_EAP_RESP

IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: R_PROC_EAP
EV_PROC_MSG
IKEv2−PROTO−2: (6): ***Processing EAP response***

The ASA decrypts this response, and the client says that it has received the AUTH payload in the previous packet (with the certificate) and received the first EAP request packet from the ASA. This is what the 'init' EAP response packet contains.

Received XML message below from the client
<?xml version="1.0" encoding="UTF−8"?>
<config−auth client="vpn" ***type="init"***>
<device−id>win</device−id>
<version who="vpn">3.0.1047</version>
<group−select>ASA−IKEV2</group−select>
<group−access>ASA−IKEV2</group−access>
</config−auth>
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: R_PROC_EAP
EV_RECV_EAP_AUTH

IKEv2−PROTO−5: (6): Action: Action_Null
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: R_BLD_EAP_
EV_RECV_EAP_REQ

This is the second request sent by the ASA to the client.

The EAP packet contains:

IKEv2−PROTO−2: (6): Sending EAP request

Generated XML message below
<?xml version="1.0" encoding="UTF−8"?>

********** Date : 04/23/2013 Time : 16:25:04 Type : Information

1. ***Code: request*** − This code is sent by the authenticator to the peer.
2. ***id: 2*** − The id helps match the EAP responses with the requests. Here the value is 2, which indicates it is the second packet in the exchange. This request has the 'config−auth' type of 'auth−request'; the ASA is requesting that the client send the user authentication credentials.
3. ***Length: 457*** − Length of the EAP packet includes the code, id, length, and EAP data.
4. ***EAP data***.

ENCR payload:

This payload is decrypted, and its contents are parsed as additional payloads.

<config−auth client="vpn" ***type="auth−request"***>
<version who="sg">9.0(2)8</version>
<opaque is−for="sg">
<tunnel−group>ASA−IKEV2</tunnel−group>
<config−hash>1367268141499</config−hash>
</opaque>
<csport>443</csport>
<auth id="main">
<form>
<input type="text" name="username" label="Username:"></input>
<input type="password" name="password" label="Password:"></input>
</form>
</auth>
</config−auth>
IKEv2−PROTO−3: (6): Building packet for encryption; contents are:
EAP Next payload: NONE, reserved: 0x0, length: 461
Code: request: id: 2, length: 457
Type: Unknown − 254
EAP data: 452 bytes

IKEv2−PROTO−3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x2
IKEv2−PROTO−3: ***HDR***[i:58AFF71141BA436B − r: FC696330E6B94D7F]
IKEv2−PROTO−4: IKEV2 HDR ispi: 58AFF71141BA436B − rspi: FC696330E6B94D7F
IKEv2−PROTO−4: Next payload: ENCR, version: 2.0
IKEv2−PROTO−4: Exchange type: IKE_AUTH, flags: ***RESPONDER MSG−RESPONSE***
IKEv2−PROTO−4: Message id: 0x2, length: 524
ENCR Next payload: EAP, reserved: 0x0, length: 496
Encrypted data: 492 bytes

IKEv2−PLAT−4: ***SENT PKT [IKE_AUTH]*** [10.0.0.1]:4500−>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000002
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: R_BLD_EAP_REQ Event: EV_START_TMR

Source : acvpnui

Description : Function: SDIMgr::ProcessPromptData File: .\SDIMgr.cpp Line: 281 Authentication type is not SDI.
****
Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpnui

Description : Function: ConnectMgr::userResponse File: .\ConnectMgr.cpp Line: 985 ***Processing user response.***
****

IKEv2−PROTO−3: (6): ***Starting timer to wait for user auth message*** (120 sec)
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: R_WAIT_EAP_RESP Event: EV_NO_EVENT

Client sends another IKE_AUTH initiator message with the EAP payload.

IKEv2−PLAT−4: RECV PKT [IKE_AUTH] [192.168.1.1]:25171−>[10.0.0.1]: InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2−PROTO−3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id
IKEv2−PROTO−3: HDR[i:58AFF71141BA436B − r: FC696330E6B94D7F]
IKEv2−PROTO−4: IKEV2 HDR ispi: 58AFF71141BA436B − rspi: FC696330
IKEv2−PROTO−4: Next payload: ENCR, version: 2.0
IKEv2−PROTO−4: ***Exchange type: IKE_AUTH, flags: INITIATOR***
IKEv2−PROTO−4: Message id: 0x3, length: 492
IKEv2−PROTO−5: (6): Request has mess_id 3; expected 3 through 3

The EAP packet contains:

1. ***Code: response*** − This code is sent by the peer to the authenticator in response to the EAP request.
2. ***id: 2*** − The id helps match the EAP responses with the requests. Here the value is 2, which indicates that this is a response to the request previously sent by the ASA (authenticator).
3. ***Length: 420*** − Length of the EAP packet includes the code, id, length, and EAP data.
4. ***EAP data***.

REAL Decrypted packet:Data: 424 bytes
EAP Next payload: NONE, reserved: 0x0, length: 424
Code: response: id: 2, length: 420
Type: Unknown − 254
EAP data: 415 bytes

The ASA processes this response. The client had requested that the user enter credentials. This EAP response has the 'config−auth' type of 'auth−reply.' This packet contains the credentials entered by the user.

Decrypted packet:Data: 492 bytes
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: R_WAIT_EAP EV_RECV_AUTH
IKEv2−PROTO−3: (6): Stopping timer to wait for auth message
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: R_WAIT_EAP EV_RECV_EAP_RESP
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: R_PROC_EAP EV_PROC_MSG
IKEv2−PROTO−2: (6): ***Processing EAP response***

Received XML message below from the client
<?xml version="1.0" encoding="UTF−8"?>
<config−auth client="vpn" ***type="auth−reply"***>
<device−id>win</device−id>
<version who="vpn">3.0.1047</version>
<session−token></session−token>
<session−id></session−id>
<opaque is−for="sg">
<tunnel−group>***ASA−IKEV2***</tunnel−group>
<config−hash>1367268141499</config−hash></opaque>
<auth>

<password>cisco123</password>
<username>Anu</username></auth>
</config−auth>
IKEv2−PLAT−1: ***EAP:Initiated User Authentication***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: R_PROC_EAP
EV_NO_EVENT
IKEv2−PLAT−5: EAP:In AAA callback
Retrieved Server Cert Digest: DACE1C274785F28BA11D64453096BAE294A
IKEv2−PLAT−5: ***EAP:success in AAA callback***
IKEv2−PROTO−3: Received response from authenticator
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: R_PROC_EAP
EV_RECV_EAP_AUTH
IKEv2−PROTO−5: (6): Action: Action_Null

The ASA builds a third EAP request in the exchange.

IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: R_BLD_EAP_
EV_RECV_EAP_REQ

The EAP packet contains:

IKEv2−PROTO−2: (6): Sending EAP request

1. ***Code: request*** − This code is sent by the authenticator to the peer.
2. ***id: 3*** − The id helps match the EAP responses with the requests. Here the value is 3, which indicates it is the third packet in the exchange. This packet has the 'config−auth' type of 'complete'; the ASA has received a reply, and the EAP exchange is complete.
3. ***Length: 4235*** − Length of the EAP packet includes the code, id, length, and EAP data.
4. ***EAP data***.

Generated XML message below
<?xml version="1.0" encoding="UTF−8"?>
<config−auth client="vpn" ***type="complete"***>
<version who="sg">9.0(2)8</version>
<session−id>32768</session−id>
<session−token>18wA0TtGmDxPKPQCJywC7fB7EWLCEgz−ZtjYpAyXx2yJ
<auth id="success">
<message id="0" param1="" param2=""></message>
</auth>

IKEv2−PROTO−3: (6): Building packet for encryption; contents are:
EAP Next payload: NONE, reserved: 0x0, length: 4239
Code: request: id: 3, length: 4235
Type: Unknown − 254
EAP data: 4230 bytes

ENCR payload:

This payload is decrypted, and its contents are parsed as additional payloads.

IKEv2−PROTO−3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id
IKEv2−PROTO−3: HDR[i:58AFF71141BA436B − r: FC696330E6B94D7F]
IKEv2−PROTO−4: IKEV2 HDR ispi: 58AFF71141BA436B − rspi: FC696330
IKEv2−PROTO−4: Next payload: ENCR, version: 2.0
IKEv2−PROTO−4: Exchange type: IKE_AUTH, flags: ***RESPONDER MSG−R***
IKEv2−PROTO−4: Message id: 0x3, length: 4300
ENCR Next payload: EAP, reserved: 0x0, length: 4272
Encrypted data:4268 bytes

IKEv2−PROTO−5: (6): Fragmenting packet, Fragment MTU: 544, ***Number of f***
Fragment ID: 2
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000003

IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: R_BLD_EAP_
EV_START_TMR
IKEv2−PROTO−3: (6): Starting timer to wait for user auth message (120 sec)
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: R_WAIT_EAP
EV_NO_EVENT

****

Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpnagent

Description : ***Current Profile: Anyconnect−ikev2.xml***
Received VPN Session Configuration Settings:
Keep Installed: enabled
Proxy Setting: do not modify
Proxy Server: none
Proxy PAC URL: none
Proxy Exceptions: none
Proxy Lockdown: enabled
Split Exclude: local LAN access preference is disabled
Split Include: disabled
Split DNS: disabled
Local LAN Wildcard: local LAN access preference is disabled
Firewall Rules: none
Client Address: 10.2.2.1
Client Mask: 255.0.0.0
Client IPv6 Address: unknown
Client IPv6 Mask: unknown
MTU: 1406
IKE Keep Alive: 20 seconds
IKE DPD: 30 seconds
Session Timeout: 0 seconds
Disconnect Timeout: 1800 seconds
Idle Timeout: 1800 seconds
Server: unknown
MUS Host: unknown
DAP User Message: none
Quarantine State: disabled
Always On VPN: not disabled
Lease Duration: 0 seconds

Default Domain: unknown
Home page: unknown
Smart Card Removal Disconnect: enabled
License Response: unknown
****

The client sends the initiator packet with the EAP payload.

IKEv2−PLAT−4: ***RECV PKT*** [IKE_AUTH] [192.168.1.1]:25171−>[10.0.0.1]:
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000004
IKEv2−PROTO−3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id
IKEv2−PROTO−3: HDR[i:58AFF71141BA436B − r: FC696330E6B94D7F]
IKEv2−PROTO−4: IKEV2 HDR ispi: 58AFF71141BA436B − rspi: FC696330
IKEv2−PROTO−4: Next payload: ENCR, version: 2.0
IKEv2−PROTO−4: ***Exchange type: IKE_AUTH, flags: INITIATOR***
IKEv2−PROTO−4: Message id: 0x4, length: 252
IKEv2−PROTO−5: (6): Request has mess_id 4; expected 4 through 4

The EAP packet contains:

1. ***Code: response*** − This code is sent by the peer to the authenticator in response to the EAP request.
2. ***id: 3*** − The id helps match the EAP responses with the requests. Here the value is 3, which indicates that this is a response to the request previously sent by the ASA (authenticator). The ASA now receives the response packet from the client, which has the 'config−auth' type of 'ack'; this response acknowledges the EAP 'complete' message sent previously by the ASA .
3. ***Length: 173*** − Length of the EAP packet includes the code, id, length, and EAP data.
4. ***EAP data***.

REAL Decrypted packet:Data: 177 bytes
EAP Next payload: NONE, reserved: 0x0, length: 177
Code: response: id: 3, length: 173
Type: Unknown − 254
EAP data: 168 bytes

The ASA processes this packet. The EAP exchange is successful. The ASA prepares to send the tunnel−group configuration in the next packet, which was previously requested by the client in the IDi payload. The ASA receives the response packet from the client, which has the 'config−auth' type of 'ack'. This response acknowledges the EAP 'complete' message that was sent by the ASA previously.

Decrypted packet:Data:252 bytes
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: R_WAIT_EAP
EV_RECV_AUTH
IKEv2−PROTO−3: (6): Stopping timer to wait for auth message
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: R_WAIT_EAP
EV_RECV_EAP_RESP
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: R_PROC_EAP
EV_PROC_MSG
IKEv2−PROTO−2: (6): ***Processing EAP response***

Received XML message below from the client
<?xml version="1.0" encoding="UTF−8"?>
<config−auth client="vpn" ***type="ack"***>
<device−id>win</device−id>
<version who="vpn">3.0.1047</version>
</config−auth>

Relevant Configuration:

```
tunnel-group ASA-IKEV2
 type remote-access
tunnel-group ASA-IKEV2
 general-attributes
 address-pool webvpn1
 authorization-server-group
 LOCAL default-group-policy
  ASA-IKEV2
tunnel-group ASA-IKEV2
 webvpn-attributes
 group-alias ASA-IKEV2
 enable
```

The EAP exchange is now successful.

The EAP packet contains:

1. ***Code***: ***success*** − This code is sent by the authenticator to the peer after completion of an EAP authentication method. This indicates that the peer has authenticated successfully to the authenticator.
2. ***id: 3*** − The id helps match the EAP responses with the requests. Here the value is 3, which indicates that this is a response to the request previously sent by the ASA (authenticator). The third set of packets in the exchange was successful, and the EAP exchange is successful.
3. ***Length: 4*** − Length of the EAP packet includes the code, id, length, and EAP data.
4. ***EAP data***.

Since the EAP exchange is successful, the client sends the IKE_AUTH initiator packet with the AUTH payload. The AUTH payload is generated from the shared secret key.

IKEv2−PLAT−3: (6) aggrAuthHdl set to 0x2000
IKEv2−PLAT−3: (6) ***tg_name set to: ASA−IKEV2***
IKEv2−PLAT−3: (6) ***tunn grp type set to: RA***
IKEv2−PLAT−1: ***EAP:Authentication successful***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: R_PROC_EAP EV_RECV_EAP_SUCCESS
IKEv2−PROTO−2: (6): Sending EAP status message
IKEv2−PROTO−3: (6): Building packet for encryption; contents are:
EAP Next payload: NONE, reserved: 0x0, length: 8
Code: success: id: 3, length: 4

IKEv2−PROTO−3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id
IKEv2−PROTO−3: HDR[i:58AFF71141BA436B − r: FC696330E6B94D7F]
IKEv2−PROTO−4: IKEV2 HDR ispi: 58AFF71141BA436B − rspi: FC696330
IKEv2−PROTO−4: Next payload: ENCR, version: 2.0
IKEv2−PROTO−4: Exchange type: IKE_AUTH, flags: RESPONDER MSG−
IKEv2−PROTO−4: Message id: 0x4, length: 76
ENCR Next payload: EAP, reserved: 0x0, length: 48
Encrypted data:44 bytes

IKEv2−PLAT−4: ***SENT PKT [IKE_AUTH]*** [10.0.0.1]:4500−>[192.168.1.1]:25 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000004

IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: R_PROC_EAP EV_START_TMR
IKEv2−PROTO−3: (6): Starting timer to wait for auth message (30 sec)
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: ***R_WAIT_EAP_AUTH_VERIFY*** Event: EV_NO_EVENT

IKEv2−PLAT−4: RECV PKT [IKE_AUTH] [192.168.1.1]:25171−>[10.0.0.1]: InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2−PROTO−3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id
IKEv2−PROTO−3: HDR[i:58AFF71141BA436B − r: FC696330E6B94D7F]
IKEv2−PROTO−4: IKEV2 HDR ispi: 58AFF71141BA436B − rspi: FC696330
IKEv2−PROTO−4: Next payload: ENCR, version: 2.0
IKEv2−PROTO−4: Exchange type: IKE_AUTH, ***flags: INITIATOR***

IKEv2−PROTO−4: Message id: 0x5, length: 92
IKEv2−PROTO−5: (6): Request has mess_id 5; expected 5 through 5

REAL Decrypted packet:Data:28 bytes
AUTH Next payload: NONE, reserved: 0x0, length: 28
Auth method PSK, reserved: 0x0, reserved 0x0
Auth data: 20 bytes

When EAP authentication is specified or
implied by the client profile and the profile does not contain the <IKEIdentity> element, the client sends
an ID_GROUP type IDi payload with the fixed string
$AnyConnectClient$.

The ASA processes this message.

Relevant Configuration:

```
crypto dynamic−map dynmap 1000
 set ikev2 ipsec−proposal 3des
crypto map crymap 10000
 ipsec−isakmp dynamic dynmap
crypto map crymap interface
 outside
```

Decrypted packet:Data: 92 bytes
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
R_WAIT_EAP_AUTH_VERIFY Event: EV_RECV_AUTH
IKEv2−PROTO−3: (6): Stopping timer to wait for auth message
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_VERIFY_A
EV_GET_EAP_KEY
IKEv2−PROTO−2: (6): Send AUTH, to verify peer after EAP exchange
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_VERIFY_A
EV_VERIFY_AUTH
IKEv2−PROTO−3: (6): ***Verify authentication data***
IKEv2−PROTO−3: (6): ***Use preshared key for id *$AnyConnectClient$*, key***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_VERIFY_A
EV_GET_CONFIG_MODE
IKEv2−PLAT−3: Config mode reply queued
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_VERIFY_A
EV_NO_EVENT
IKEv2−PLAT−3: PSH: client=AnyConnect client−version=3.0.1047 client−os=
client−os−version=
IKEv2−PLAT−3: Config mode reply completed
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_VERIFY_A
EV_OK_GET_CONFIG
IKEv2−PROTO−3: (6): Have config mode data to send
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_VERIFY_A
EV_CHK4_IC
IKEv2−PROTO−3: (6): Processing initial contact
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_VERIFY_A
EV_CHK_REDIRECT
IKEv2−PROTO−5: (6): Redirect check is already done for this session, skipping
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_VERIFY_A
EV_PROC_SA_TS
IKEv2−PROTO−2: (6): ***Processing auth message***
IKEv2−PLAT−1: ***Crypto Map: Map dynmap seq 1000. Adjusted selector using***
IKEv2−PLAT−3: ***Crypto Map: match on dynamic map dynmap seq 1000***
IKEv2−PLAT−3: PFS disabled for RA connection
IKEv2−PROTO−3: (6):
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_VERIFY_A

EV_NO_EVENT
IKEv2−PLAT−2: Received PFKEY SPI callback for SPI 0x30B848A4, error FA
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_VERIFY_A
EV_OK_RECD_IPSEC_RESP

IKEv2−PROTO−2: (6): ***Processing auth message***

The ASA builds the IKE_AUTH response message with the SA, TSi, and TSr payloads.

IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: ***R_BLD_AUTH***
EV_MY_AUTH_METHOD
IKEv2−PROTO−3: (6): ***Get my authentication method***

The IKE_AUTH responder packet contains:

1. ***ISAKMP Header*** − SPI/version/flags.
2. ***AUTH payload*** − With the chosen authentication method.
3. ***CFG*** − CFG_REQUEST/ CFG_REPLY allows an IKE endpoint to request information from its peer. If an attribute in the CFG_REQUEST configuration payload is not zero−length, it is taken as a suggestion for that attribute. The CFG_REPLY configuration payload may return that value or a new one. It may also add new attributes and not include some requested ones. Requestors ignore returned attributes that they do not recognize. The ASA replies to the client with the tunnel configuration atrributes in the CFG_REPLY packet.
4. ***SAr2*** − SAr2 initiates the SA, which is similar to the phase 2 transform set exchange in IKEv1.
5. ***TSi*** and ***TSr*** − The initiator and responder traffic selectors contain, respectively, the source and destination address of the initiator and responder in order to forward and receive encrypted traffic. The address range specifies that all traffic to and from that range is

IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_BLD_AUTH
EV_GET_PRESHR_KEY
IKEv2−PROTO−3: (6): ***Get peer's preshared key for *$AnyConnectClient$****
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_BLD_AUTH
EV_GEN_AUTH
IKEv2−PROTO−3: (6): ***Generate my authentication data***
IKEv2−PROTO−3: (6): ***Use preshared key for id hostname=ASA−IKEV2, key***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_BLD_AUTH
EV_CHK4_SIGN
IKEv2−PROTO−3: (6): Get my authentication method
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_BLD_AUTH
EV_OK_AUTH_GEN
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_BLD_EAP_
Event: EV_GEN_AUTH
IKEv2−PROTO−3: (6): Generate my authentication data
IKEv2−PROTO−3: (6): Use preshared key for id hostname=ASA−IKEV2, key
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: R_BLD_EAP_
Event: EV_SEND_AUTH
IKEv2−PROTO−2: (6): ***Send AUTH, to verify peer after EAP exchange***
IKEv2−PROTO−3: ESP Proposal: 1, SPI size: 4 (IPSec negotiation),
Num. transforms: 3
 AES−CBC SHA96
IKEv2−PROTO−5: Construct Notify Payload: ESP_TFC_NO_SUPPORTIKEv
Construct Notify Payload: NON_FIRST_FRAGSIKEv2−PROTO−3: (6): Build
encryption; contents are:
AUTH Next payload: CFG, reserved: 0x0, length: 28
Auth method PSK, reserved: 0x0, reserved 0x0
Auth data: 20 bytes
CFG Next payload: SA, reserved: 0x0, length: 4196
cfg type: ***CFG_REPLY,*** reserved: 0x0, reserved: 0x0

attrib type: internal IP4 address, length: 4

01 01 01 01
attrib type: internal IP4 netmask, length: 4

00 00 00 00

tunneled. If the proposal is acceptable to the responder, it sends identical TS payloads back.

ENCR payload:

This payload is decrypted, and its contents are parsed as additional payloads.

attrib type: internal address expiry, length: 4

00 00 00 00
attrib type: application version, length: 16

41 53 41 20 31 30 30 2e 37 28 36 29 31 31 36 00
attrib type: Unknown − 28704, length: 4

00 00 00 00
attrib type: Unknown − 28705, length: 4

00 00 07 08
attrib type: Unknown − 28706, length: 4

00 00 07 08
attrib type: Unknown − 28707, length: 1

01
attrib type: Unknown − 28709, length: 4

00 00 00 1e
attrib type: Unknown − 28710, length: 4

00 00 00 14
attrib type: Unknown − 28684, length: 1

01
attrib type: Unknown − 28711, length: 2

05 7e
attrib type: Unknown − 28679, length: 1

00
attrib type: Unknown − 28683, length: 4

80 0b 00 01
attrib type: Unknown − 28725, length: 1

00
attrib type: Unknown − 28726, length: 1

00
attrib type: Unknown − 28727, length: 4056

3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31
2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54
46 2d 38 22 3f 3e 3c 63 6f 6e 66 69 67 2d 61 75
74 68 20 63 6c 69 65 6e 74 3d 22 76 70 6e 22 20
74 79 70 65 3d 22 63 6f 6d 70 6c 65 74 65 22 3e
3c 76 65 72 73 69 6f 6e 20 77 68 6f 3d 22 73 67
22 3e 31 30 30 2e 37 28 36 29 31 31 36 3c 2f 76
65 72 73 69 6f 6e 3e 3c 73 65 73 73 69 6f 6e 2d
69 64 3e 38 31 39 32 3c 2f 73 65 73 73 69 6f 6e
<snip>

72 6f 66 69 6c 65 2d 6d 61 6e 69 66 65 73 74 3e
3c 2f 63 6f 6e 66 69 67 3e 3c 2f 63 6f 6e 66 69
67 2d 61 75 74 68 3e 00
attrib type: Unknown − 28729, length: 1

00
SA Next payload: TSi, reserved: 0x0, length: 44
IKEv2−PROTO−4: last proposal: 0x0, reserved: 0x0, length: 40
Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES−CBC
IKEv2−PROTO−4: last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
IKEv2−PROTO−4: last transform: 0x0, reserved: 0x0: length: 8
type: 5, reserved: 0x0, id:

TSi Next payload: TSr, reserved: 0x0, length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 10.2.2.1, end addr: 10.2.2.1
TSr Next payload: NOTIFY, reserved: 0x0, length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 0.0.0.0, end addr: 255.255.255.255

IKEv2−PROTO−3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id
IKEv2−PROTO−3: HDR[i:58AFF71141BA436B − r: FC696330E6B94D7F]
IKEv2−PROTO−4: IKEV2 HDR ispi: 58AFF71141BA436B − rspi: FC696330
IKEv2−PROTO−4: Next payload: ENCR, version: 2.0
IKEv2−PROTO−4: ***Exchange type: IKE_AUTH, flags: RESPONDER MSG−***
IKEv2−PROTO−4: Message id: 0x5, length: 4396
ENCR Next payload: AUTH, reserved: 0x0, length: 4368
Encrypted data: 4364 bytes

The ASA sends out this IKE_AUTH response message, which is fragmented into nine packets. The IKE_AUTH exchange is complete.

IKEv2−PROTO−5: (6): Fragmenting packet, Fragment MTU: 544, ***Number of***
Fragment ID: 3
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2−PLAT−4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500−>[192.168.1.1]:25

InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: AUTH_DONE
IKEv2−PROTO−5: (6): Action: Action_Null
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: ***AUTH_DONE***
EV_PKI_SESH_CLOSE
****
Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpnagent

Description : Function: ikev2_log
File: .\ikev2_anyconnect_osal.cpp
Line: 2730
The IPsec connection has been established.
****
Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpnagent

Description : IPsec session registration:
Encryption: AES−CBC
PRF: SHA1
HMAC: SHA96
Local auth method: PSK
Remote auth method: PSK
Sequence id: 0
Key size: 192
DH group: 1
Rekey time: 4294967 seconds
Local address: 192.168.1.1
Remote address: 10.0.0.1
Local port: 4500
Remote port: 4500
Session id: 1
****
Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpnui

Description : ***The profile configured on the secure gateway is: Anyconnect−ik***
****
Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpnui

Description : Message type information sent to the user:
Establishing VPN session...
****

−−−−−−−−−−−−−−−−−−−−−−−−−−−IKE_AUTH exchange ends−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

****

Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpndownloader

Description : Function: ProfileMgr::loadProfiles
File: ..\Api\ProfileMgr.cpp
Line: 148
Loaded profiles:
C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConne
Mobility Client\Profile\anyconnect−ikev2.xml

****

****

Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpndownloader

Description : Current Preference Settings:
ServiceDisable: false
CertificateStoreOverride: false
CertificateStore: All
ShowPreConnectMessage: false
AutoConnectOnStart: false
MinimizeOnConnect: true
LocalLanAccess: false
AutoReconnect: true
AutoReconnectBehavior: DisconnectOnSuspend
UseStartBeforeLogon: false
AutoUpdate: true
RSASecurIDIntegration: Automatic
WindowsLogonEnforcement: SingleLocalLogon
WindowsVPNEstablishment: LocalUsersOnly
ProxySettings: Native
AllowLocalProxyConnections: true
PPPExclusion: Disable
PPPExclusionServerIP:
AutomaticVPNPolicy: false
TrustedNetworkPolicy: Disconnect
UntrustedNetworkPolicy: Connect
TrustedDNSDomains:
TrustedDNSServers:
AlwaysOn: false
ConnectFailurePolicy: Closed
AllowCaptivePortalRemediation: false
CaptivePortalRemediationTimeout: 5
ApplyLastVPNLocalResourceRules: false
AllowVPNDisconnect: true
EnableScripting: false
TerminateScriptOnNextEvent: false
EnablePostSBLOnConnectScript: true

AutomaticCertSelection: true
RetainVpnOnLogoff: false
UserEnforcement: SameUserOnly
EnableAutomaticServerSelection: false
AutoServerSelectionImprovement: 20
AutoServerSelectionSuspendTime: 4
AuthenticationTimeout: 12
SafeWordSofTokenIntegration: false
AllowIPsecOverSSL: false
ClearSmartcardPin: true
****

Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpnui

Description : Message type information sent to the user:
Establishing VPN − Examining system...
****

Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpnui

Description : Message type information sent to the user:
Establishing VPN − Activating VPN adapter...
****

Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpnagent

Description : Function: CVirtualAdapter::DoRegistryRepair
File: .\WindowsVirtualAdapter.cpp
Line: 1869
Found VA Control key: SYSTEM\CurrentControlSet\ENUM\ROOT\NET\0000

****

Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpnagent

Description : ***A new network interface has been detected.***
****

Date : 04/23/2013
Time : 16:25:07
Type : Information
Source : acvpnagent

Description : Function: CRouteMgr::logInterfaces
File: .\RouteMgr.cpp
Line: 2076
Invoked Function: logInterfaces

Return Code: 0 (0x00000000)
Description: IP Address Interface List:
10.2.2.1
192.168.1.1
****
Date : 04/23/2013
Time : 16:25:08
Type : Information
Source : acvpnagent

Description : Host Configuration:
Public address: 192.168.1.1
Public mask: 255.255.255.0
Private Address: 10.2.2.1
Private Mask: 255.0.0.0
Private IPv6 Address: N/A
Private IPv6 Mask: N/A
Remote Peers: 10.0.0.1 (TCP port 443, UDP port 500), 10.0.0.1 (UDP port 45
Private Networks: none
Public Networks: none
Tunnel Mode: yes
****

The connection is entered into the Security Association (SA) database, and the status is REGISTERED. The ASA also performs some checks like Common Access Card (CAC) stats, presence of duplicate SAs, and sets values like dead peer detection (DPD) and so forth.

IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: AUTH_DONE ***EV_INSERT_IKE***
IKEv2−PROTO−2: (6): ***SA created; inserting SA into database***
IKEv2−PLAT−3:
CONNECTION STATUS: UP... peer: 192.168.1.1:25171, phase1_id: *$AnyCo
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: AUTH_DONE ***EV_REGISTER_SESSION***
IKEv2−PLAT−3: (6) ***username set to: Anu***
IKEv2−PLAT−3:
CONNECTION STATUS: REGISTERED... peer: 192.168.1.1:25171, ***phase1_ *$AnyConnectClient$****
IKEv2−PROTO−3: (6): Initializing DPD, configured for 10 seconds
IKEv2−PLAT−3: (6) mib_index set to: 4501
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: AUTH_DONE EV_GEN_LOAD_IPSEC
IKEv2−PROTO−3: (6): Load IPSEC key material
IKEv2−PLAT−3: Crypto Map: match on dynamic map dynmap seq 1000
IKEv2−PLAT−3: (6) ***DPD Max Time will be: 30***
IKEv2−PLAT−3: (6) ***DPD Max Time will be: 30***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: AUTH_DONE EV_START_ACCT
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: AUTH_DONE EV_CHECK_DUPE
IKEv2−PROTO−3: (6): ***Checking for duplicate SA***
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: AUTH_DONE EV_CHK4_ROLE

IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: READY Event
EV_R_UPDATE_CAC_STATS
IKEv2−PLAT−5: New ikev2 sa request activated
IKEv2−PLAT−5: Decrement count for incoming negotiating
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: READY Event
IKEv2−PROTO−3: (6): Starting timer to delete negotiation context
IKEv2−PROTO−5: (6): SM Trace−> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: READY Event
EV_NO_EVENT
IKEv2−PLAT−2: Received PFKEY add SA for SPI 0x77EE5348, error FALSE
IKEv2−PLAT−2: Received PFKEY update SA for SPI 0x30B848A4, error FAI
****
Date : 04/23/2013
Time : 16:25:08
Type : Information
Source : acvpnagent

Description : ***The VPN connection has been established and can now pass dat***
****
Date : 04/23/2013
Time : 16:25:08
Type : Information
Source : acvpnui

Description : Message type information sent to the user:
Establishing VPN − Configuring system...
****
Date : 04/23/2013
Time : 16:25:08
Type : Information
Source : acvpnui

Description : Message type information sent to the user:
Establishing VPN...
****
Date : 04/23/2013
Time : 16:25:37
Type : Information
Source : acvpnagent

File: .\IPsecProtocol.cpp
Line: 945
IPsec tunnel is established
****

Tunnel Verification

AnyConnect

Sample output from the ***show vpn-sessiondb detail anyconnect*** command is:

```
Session Type: AnyConnect Detailed

   Username     : Anu                    Index        : 2
   Assigned IP  : 10.2.2.1                Public IP    : 192.168.1.1
   Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
   License      : AnyConnect Premium
   Encryption   : AES192 AES256          Hashing      : none SHA1 SHA1
   Bytes Tx     : 0                      Bytes Rx     : 11192
   Pkts Tx      : 0                      Pkts Rx      : 171
   Pkts Tx Drop : 0                      Pkts Rx Drop : 0
   Group Policy : ASA-IKEV2              Tunnel Group : ASA-IKEV2
   Login Time   : 22:06:24 UTC Mon Apr 22 2013
   Duration     : 0h:02m:26s
   Inactivity   : 0h:00m:00s
   NAC Result   : Unknown
   VLAN Mapping : N/A                    VLAN         : none

   IKEv2 Tunnels: 1
   IPsecOverNatT Tunnels: 1
   AnyConnect-Parent Tunnels: 1

   AnyConnect-Parent:
     Tunnel ID    : 2.1
     Public IP    : 192.168.1.1
     Encryption   : none                   Auth Mode    : userPassword
   Idle Time Out: 30 Minutes             Idle TO Left : 27 Minutes
   Client Type  : AnyConnect
   Client Ver   : 3.0.1047
    IKEv2:
     Tunnel ID    : 2.2
     UDP Src Port : 25171                  UDP Dst Port : 4500
     Rem Auth Mode: userPassword
     Loc Auth Mode: rsaCertificate
     Encryption   : AES192                 Hashing      : SHA1
     Rekey Int (T): 86400 Seconds          Rekey Left(T): 86254 Seconds
     PRF          : SHA1                   D/H Group    : 1
     Filter Name  :
     Client OS    : Windows
    IPsecOverNatT:
     Tunnel ID    : 2.3
     Local Addr   : 0.0.0.0/0.0.0.0/0/0
     Remote Addr  : 10.2.2.1/255.255.255.255/0/0
     Encryption   : AES256                 Hashing      : SHA1
   Encapsulation: Tunnel
   Rekey Int (T): 28800 Seconds          Rekey Left(T): 28654 Seconds
   Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4607990 K-Bytes
   Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
   Bytes Tx     : 0                      Bytes Rx     : 11192
   Pkts Tx      : 0                      Pkts Rx      : 171
    NAC:
     Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
     SQ Int (T)   : 0 Seconds              EoU Age(T)   : 146 Seconds
     Hold Left (T): 0 Seconds              Posture Token:
    Redirect URL :
```

ISAKMP

Sample output from the ***show crypto ikev2 sa*** command is:

```
ASA-IKEV2#  show crypto ikev2 sa
```

```
      IKEv2 SAs:

      Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

      Tunnel-id                Local                Remote     Status         Role
       55182129    10.0.0.1/4500         192.168.1.1/25171      READY    RESPONDER
            Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
            Life/Active Time: 86400/112 sec
      Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
                remote selector 10.2.2.1/0 - 10.2.2.1/65535
              ESP spi in/out: 0x30b848a4/0x77ee5348
```

Sample output from the ***show crypto ikev2 sa detail*** command is:

```
ASA-IKEV2# show crypto ikev2 sa detail

    IKEv2 SAs:

    Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

    Tunnel-id                Local                Remote     Status         Role
     55182129    10.0.0.1/4500         192.168.1.1/25171      READY    RESPONDER
       Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
         Life/Active Time: 86400/98 sec
         Session-id: 2
         Status Description: Negotiation done
         Local spi: FC696330E6B94D7F       Remote spi: 58AFF71141BA436B
         Local id: hostname=ASA-IKEV2
         Remote id: *$AnyConnectClient$*
         Local req mess id: 0              Remote req mess id: 9
         Local next mess id: 0             Remote next mess id: 9
         Local req queued: 0               Remote req queued: 9
         Local window: 1                   Remote window: 1
         DPD configured for 10 seconds, retry 2
         NAT-T is detected  outside
         Assigned host addr: 10.2.2.1
   Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
             remote selector 10.2.2.1/0 - 10.2.2.1/65535
             ESP spi in/out: 0x30b848a4/0x77ee5348
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
            Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
            ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

IPSec

Sample output from the ***show crypto ipsec sa*** command is:

```
ASA-IKEV2# show crypto ipsec sa
   interface: outside
       Crypto map tag: dynmap, seq num: 1000, local addr: 10.0.0.1

     local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
        remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0)
        current_peer: 192.168.1.1, username: Anu
        dynamic allocated peer ip: 10.2.2.1

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
         #pkts decaps: 163, #pkts decrypt: 108, #pkts verify: 108
         #pkts compressed: 0, #pkts decompressed: 0
         #pkts not compressed: 0, #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: 55

 local crypto endpt.: 10.0.0.1/4500, remote crypto endpt.: 192.168.1.1/25171
    path mtu 1488, ipsec overhead 82, media mtu 1500
    current outbound spi: 77EE5348
    current inbound spi : 30B848A4

inbound esp sas:
    spi: 0x30B848A4 (817383588)
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={RA, Tunnel,  NAT-T-Encaps, }
       slot: 0, conn_id: 8192, crypto-map: dynmap
       sa timing: remaining key lifetime (sec): 28685
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
       0xFFAD6BED 0x7ABFD5BF
  outbound esp sas:
    spi: 0x77EE5348 (2012107592)
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={RA, Tunnel,  NAT-T-Encaps, }
       slot: 0, conn_id: 8192, crypto-map: dynmap
       sa timing: remaining key lifetime (sec): 28685
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
      0x00000000 0x00000001
```

Related Information

- ***RFC 4306, Internet Key Exchange (IKEv2) Protocol***
- ***RFC 3748, Extensible Authentication Protocol (EAP)***
- ***RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2)***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Oct 09, 2013 Document ID: 116158