適用於遠端訪問VPN的ASA IKEv2調試故障排除

目錄

簡介

本文檔介紹當網際網路金鑰交換版本2(IKEv2)與Cisco AnyConnect安全移動客戶端一起使用時，如何理解思科自適應安全裝置(ASA)上的調試。本文檔還提供了有關如何在ASA配置中轉換特定調試行的資訊。

本文檔不介紹在建立VPN隧道後如何向ASA傳遞流量，也不包括IPSec或IKE的基本概念。

必要條件

需求

思科建議您瞭解IKEv2的資料包交換。有關詳細資訊，請參閱IKEv2資料包交換和協定級別調試。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 網際網路金鑰交換版本2(IKEv2)

- Cisco Adaptive Security Appliance(ASA)版本8.4或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

核心問題

Cisco技術援助中心(TAC)通常使用IKE和IPSec debug命令來瞭解IPSec VPN隧道建立存在問題的位置，但這些命令可能是隱性的。

案例

Debug指令

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

ASA配置

此ASA配置是嚴格意義上的基本配置，不使用外部伺服器。

```
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檔案

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

附註：XML客戶端配置檔案中的UserGroup名稱必須與ASA上隧道組的名稱相同。否則，錯誤消息'Invalid Host Entry.在AnyConnect客戶端上顯示「請重新輸入」。

調試日誌和說明

附註：診斷和報告工具(DART)中的日誌通常非常簡潔，因此本示例中由於無關緊要而省略了某些DART日誌。

伺服器消息說明

ASA從客戶端接收IKE_SA_INIT消息。

第一對消息是IKE_SA_INIT交換。這些消息協商加密演算法、交換金鑰並執行Diffie-hellman(DH)交換。從客戶端收到的IKE_SA_INIT消息包含以下欄位：

1. **ISAKMP報頭**- SPI/版本/標誌。
2. **SAi1** - IKE啟動器支援的加密演算法。

3. **KEi** — 發起方的DH公鑰值。
4. **N** — 發起程式編號

ASA驗證並處理
IKE_INIT消息。ASA:

1. 從中選擇加密套件
   由發起人提供的。
2. 計算自己的DH金鑰。
3. 計算SKYID值
   所有鍵都可以派生
   此IKE_SA。所有專案的標頭
   後續消息是
   已加密且經過身份驗證。其
   用於加密和
   完整性保護已派生
   ，稱為：

   SK_e -加密。**SK_a -**身份驗證。**SK_d -**派生和使用
   用於進一步推導
   金鑰材料
   CHILD_SA。單獨的SK_e和SK_a是
   每個方向計算。

相關配置：

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

ASA為IKE_SA_INIT交換構建響應消息。
此資料包包含：

1. **ISAKMP報頭**- SPI/版本/標誌。
2. **SAr1** - IKE響應程式選擇的加密演算法。
3. **KEr** — 響應方的DH公鑰值。
4. **N** — 響應程式無。

ASA傳送IKE_SA_INIT交換的響應消息。IKE_SA_INIT交換現在已完成。ASA啟動身份驗證過程的計時器。

身份驗證使用EAP完成。在EAP會話中只允許使用一個EAP身份驗證方法。ASA從客戶端接收IKE_AUTH消

客戶端包含IDi負載時
但不是AUTH負載，這表示
客戶端已宣告身份，但
沒有證明。在偵錯中，AUTH
ike_AUTH中不存在負載
客戶端傳送的資料包。使用者端
僅在
EAP交換成功。如果ASA
願意使用
身份驗證方法，它放置一個EAP
消息4中的負載並推遲傳送
SAr2、TSi和TSr，直到啟動器
身份驗證在
後續的IKE_AUTH交換。
IKE_AUTH發起程式資料包包含：

1. **ISAKMP報頭**-
   SPI/版本/標誌。
2. **IDi** — 隧道組名稱，該隧道組名稱
   客戶端希望連線到
   可以通過IDi傳送
   型別ID_KEY_ID的負載
   的初始消息

IKE_AUTH交換。此
在客戶端配置檔案*為
使用組名稱預配置
或者，在上次成功後
驗證，使用者端具有
在其中
首選項檔案。ASA
嘗試匹配隧道組
包含IKE內容的名稱
IDi負載。在第一個之後
成功的IPSec VPN是
已建立，客戶端快取
組名稱（組別名）
使用者已驗證。此組
名稱在IDi中提供
下一個連線的負載
嘗試指示
可能的目標組
使用者。當EAP身份驗證為
由客戶端指定或暗示
配置檔案和
包含<IKEIdentity>
元素，客戶端傳送
ID_GROUP型別IDi負載
使用固定字串
$AnyConnectClient$。

3. CERTREQ — 客戶端為
請求ASA
首選證書。憑證
可能包括請求負載
在交換中
需要獲取
接收器。證書請求
負載的處理者
檢查「證書編碼」
欄位以確定
處理器是否有任何
此型別的證書。如果是，
「證書頒發機構」欄位為
檢查，以確定是否
處理器具有任何憑證
最多可以驗證其中一個
指定的證書
當局。這可能是一條鏈
憑證。
4. CFG - CFG_REQUEST/
CFG_REPLY允許IKE

請求資訊的終結點
從同伴那裡。如果
CFG_REQUEST配置
負載不是零長度，它是
作為建議提出
attribute.CFG_REPLY
配置負載可能返回
這個值還是一個新值。可以
同時新增新屬性，但不新增
包括一些請求請求。
已返回請求者忽略
不存在的屬性
認識。在這些調試中，
客戶端正在請求隧道
中的配置
CFG_REQUEST。ASA
回覆此封包並傳送通道
配置屬性僅在此之後
eap交換成功。

5. **SAi2** - SAi2啟動SA，
類似於第2階段
ikev1中的轉換集交換。
6. **TSi**和**TSr** — 發起方和
響應器流量選擇器
分別包含源
和目的地址
發起方和響應方
轉發和接收已加密
流量。地址範圍
指定所有往返流量
這個範圍是隧道式的。如果
計畫書為本集團所接受
響應方傳送相同的TS
有效載荷。

客戶機必須為其提供的屬性
組身份驗證儲存在
AnyConnect配置檔案。
***相關配置檔案配置：**

```
<ServerList>
<HostEntry>
 <HostName>Anu-IKEV2
</HostName>
 <HostAddress>10.0.0.1
</HostAddress>
```

```
<PrimaryProtocol>IPsec
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

ASA生成對IKE_AUTH消息的響應，並準備向客戶端進行身份驗證。

ASA傳送AUTH負載，以便從客戶端請求使用者憑證。ASA將AUTH方法作為「RSA」傳送，因此它將自己
由於ASA願意使用可擴展的身份驗證方法，因此ASA將EAP負載置於消息4中，並推遲傳送SAr2、TSi和TS
EAP資料包包含：

1. **代碼：request** — 此代碼由身份驗證器傳送到對等裝置。
2. **id:1** - id有助於將EAP響應與請求進行匹配。這裡的值為1，表示這是EAP交換中的第一個資料包。此
3. **長度：150** - EAP資料包的長度包括代碼、id、長度和EAP資料。
4. **EAP資料**。

如果憑證較大或包括憑證鏈結，則可能會導致分段。發起方和響應方KE有效負載還可以包括大金鑰，這也

客戶端對EAP請求作出響應。

EAP資料包包含：

1. **代碼：response** — 此代碼由對等體傳送到身份驗證器以響應EAP請求。
2. **id:1 -** id有助於將EAP響應與請求匹配。此處值為1，表示這是對ASA（身份驗證器）之前傳送的請求的
3. **長度：252** - EAP資料包的長度包括代碼、id、長度和EAP資料。
4. **EAP資料**。

ASA解密此響應，客戶端稱其已在上一個資料包（包含證書）中收到AUTH負載，並從ASA收到第一個EAP

這是ASA向客戶端傳送的第二個請求。
EAP資料包包含：

1. **代碼：request** — 此代碼由身份驗證器傳送到對等裝置。
2. **id:2** - id有助於將EAP響應與請求進行匹配。這裡的值為2，表示它是交換中的第二個資料包。此要求的
3. **長度：457** - EAP資料包的長度包括代碼、id、長度和EAP資料。
4. **EAP資料**。

增強負載：
此負載被解密，其內容被解析為附加負載。

客戶端傳送另一條包含EAP負載的IKE_AUTH啟動器消息。
EAP資料包包含：

1. **代碼：response** — 此代碼由對等體傳送到身份驗證器以響應EAP請求。
2. **id:2** - id有助於將EAP響應與請求進行匹配。此處值為2，表示這是對ASA（身份驗證器）之前傳送的請
3. **長度：420** - EAP資料包的長度包括代碼、id、長度和EAP資料。
4. **EAP資料**。

ASA處理此響應。客戶端已請求使用者輸入憑據。此EAP響應的「config-auth」型別為「auth-reply」。 此

ASA在交換中構建第三個EAP請求。
EAP資料包包含：

1. **代碼：request** — 此代碼由身份驗證器傳送到對等裝置。
2. **id:3** - id有助於將EAP響應與請求進行匹配。此處的值為3，表示它是交換中的第三個資料包。此封包
3. **長度：4235** - EAP資料包的長度包括代碼、id、長度和EAP資料。
4. **EAP資料**。

增強負載：
此負載被解密，其內容被解析為附加負載。

客戶端傳送帶有EAP負載的啟動器資料包。
EAP資料包包含：

1. **代碼：response** — 此代碼由對等體傳送到身份驗證器以響應EAP請求。
2. **id:3** - id有助於將EAP響應與請求進行匹配。此處值為3，表示這是對ASA（身份驗證器）之前傳送的請
3. **長度：173** - EAP資料包的長度包括代碼、id、長度和EAP資料。
4. **EAP資料**。

ASA處理此資料包。其
EAP交換成功。ASA
準備傳送隧道組
配置下一個資料包，
之前是客戶在
IDi負載。ASA接收
來自客戶端的響應資料包，
具有「config-auth」型別的「ack」。 此
響應確認EAP
傳送的「完成」消息
ASA之前。
相關配置：

```
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
```

EAP交換現在成功。
EAP資料包包含：

1. **代碼**:success — 此代碼為
   由身份驗證器傳送到
   完成EAP後的對等體
   驗證方法。此
   表示對等體具有
   已成功驗證到
   驗證器。
2. **id:3** - ID用於匹配
   EAP響應請求。
   這裡值為3，其中
   表示這是對
   之前由傳送者
   ASA（身份驗證器）。 第三組
   交換的資料包
   成功，並且EAP交換
   成功。
3. **長度：4** - EAP的長度
   資料包包含代碼、id、
   長度和EAP資料。
4. **EAP資料**。

由於EAP交換成功，客戶端將傳送包含AUTH負載的IKE_AUTH發起程式資料包。身份驗證負載由共用金鑰

當指定EAP身份驗證或
客戶端配置檔案和
配置檔案不包含
<IKEIdentity>元素，客戶端將
ID_GROUP型別IDi負載
固定字串*$AnyConnectClient$*。
ASA處理此消息。
相關配置：

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

ASA使用SA、TSi和TSr負載構建IKE_AUTH響應消息。
IKE_AUTH響應器封包包含：

1. **ISAKMP報頭**- SPI/版本/標誌。
2. **AUTH payload** — 使用選擇的驗證方法。
3. **CFG** - CFG_REQUEST/ CFG_REPLY允許IKE端點從其對等體請求資訊。如果CFG_REQUEST配置
   的隧道配置屬性來回覆客戶端。
4. **SAr2** - SAr2啟動SA，這與IKEv1中的第2階段轉換集交換類似。
5. **TSi**和**TSr** — 發起方和響應方流量選擇器分別包含發起方和響應方的源地址和目的地址，以便轉發和

增強負載：
此負載被解密，其內容被解析為附加負載。

ASA發出此IKE_AUTH響應消息，該消息被分段為九個資料包。IKE_AUTH交換完成。

此連線已輸入安全關聯(SA)資料庫，狀態為REGISTERED。ASA還會執行一些檢查，如通用訪問卡(CAC)

通道驗證

AnyConnect

show vpn-sessiondb detail anyconnect命令的輸出示例為：

```
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

show crypto ikev2 sa命令的輸出示例為：

```
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
```

show crypto ikev2 sa detail命令的輸出示例為：

```
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

show crypto ipsec sa命令的輸出示例為：

```
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
```

相關資訊

- RFC 4306，網際網路金鑰交換(IKEv2)通訊協定
- RFC 3748，可擴充驗證通訊協定(EAP)
- RFC 5996，網際網路金鑰交換通訊協定第2版(IKEv2)
- 技術支援與文件 - Cisco Systems