

远程访问VPN故障排除的ASA IKEv2调试

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[核心问题](#)

[方案](#)

[debug 命令](#)

[ASA 配置](#)

[XML文件](#)

[调试日志和说明](#)

[通道验证](#)

[AnyConnect](#)

[ISAKMP](#)

[IPsec](#)

[相关信息](#)

简介

本文描述如何了解在思科可适应安全工具(ASA)的调试，当互联网密钥交换版本2 (IKEv2)时与Cisco AnyConnect安全移动客户端一起使用。本文在ASA配置里也提供信息关于怎样翻译某些调试线路。

本文不描述如何通过流量，在VPN通道设立了对ASA后，亦不包括IPSec或IKE基本概念。

先决条件

要求

思科建议您有信息包交换的知识IKEv2的。欲知更多信息，参考[IKEv2信息包交换和协议级调试](#)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 互联网密钥交换版本2 (IKEv2)
- Cisco可适应安全工具(ASA)版本8.4或以上

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

核心问题

Cisco技术支持中心(TAC)经常使用IKE和IPSec调试指令为了了解哪里有与IPSec VPN隧道建立的一问题，但是命令可以隐秘。

方案

debug 命令

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

ASA 配置

此ASA配置严格是基本，没有使用外部服务器。

```
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文件

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

注意：在XML客户端配置文件的用户组名称必须是相同的象隧道群的名称ASA的。否则，错误消息‘无效主机条目。请重新输入’被看到在AnyConnect客户端。

调试日志和说明

注意：从诊断和报告工具(箭)的日志通常是非常话多，因此某些箭日志在本例中省略由于无价值。

服务器消息说明

ASA收到从客户端的IKE_SA_INIT消息。

第一个对消息是IKE_SA_INIT交换。这些消息协商加密算法，交换目前，并且执行Diffie-Hellman (DH)交换。从客户端接收的IKE_SA_INIT消息包含这些字段：

1. **ISAKMP报头**- SPI/version/flags.
2. **SAi1** -该的加密算法IKE发起者支持。
3. **KEi** - DH发起者的公共密钥值。
4. **N** -发起者目前。

ASA验证并且处理
IKE_INIT消息。ASA：

1. 选择crypto套件从发起者提供的那些。
2. 计算其自己的DH密钥。
3. 计算一个SKEYID值从哪些所有密钥可以派生为此IKE_SA。所有的报头随后的消息是已加密和已验证。用于加密的密钥和完整性保护派生从SKEYID和叫作：

SK_e -加密。**SK_a** -验证。**SK_d** -派生和使用派生更加进一步
密钥材料为CHILD_SAs。分开的SK_e和SK_a是计算为每个方向。

相关配置：

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

ASA修建IKE_SA_INIT交换的响应消息。

此数据包包含：

1. **ISAKMP报头**- SPI/version/flags.
2. **SAr1** - IKE响应方选择的加密算法。
3. **KEr** - DH响应方的公共密钥值。
4. **N** -响应方目前。

ASA派出IKE_SA_INIT交换的响应消息。IKE_SA_INIT交换当前完成。ASA启动认证过程的计时器。

验证执行与EAP。仅单个EAP验证方法在EAP会话内允许。ASA收到从客户端的IKE_AUTH消息。

当客户端包括IDi有效负载
但是不是验证有效负载，这指示
客户端宣称标识，但是有
没证明它。在调试，验证
有效负载不是存在IKE_AUTH
客户端发送的数据包。客户端
在之后发送验证有效负载
EAP交换是成功的。如果ASA
是愿意使用可扩展
认证方法，它放置一个EAP
在消息4的有效负载和延迟发送
SAr2、TSi和Tsr直到发起者
验证完成在a
随后的IKE_AUTH交换。

IKE_AUTH发起者数据包包含：

1. ISAKMP报头-

SPI/version/flags.

2. IDi -组名那

客户端希望连接

可以由IDi传送

类型ID_KEY_ID有效负载

最初的消息

IKE_AUTH交换。这

当客户端profile*是，发生

预先配置与组名

或者，在一上一个成功以后

验证，客户端有

在其缓存了组名

首选文件。ASA

尝试匹配隧道群

名称以IKE的内容

IDi有效负载。在第一以后

成功的IPSec VPN是

已建立的客户端缓存

的组名(组别名)

用户验证。此组

名称在IDi传送

导航的有效负载

尝试为了指示

希望的可能的组
用户。当EAP验证是
指定或暗示由客户端
配置文件和配置文件不
包含<IKEIdentity>
元素，客户端发送
ID_GROUP类型ID有效负载
使用已修复字符串
\$AnyConnectClient\$.

3. **CERTREQ** -客户端是
请求a的ASA
首选的证书。证书
请求有效载荷可能包括
在交换，当发送方
需要获得证书
接收方。证书请求
有效负载处理由
'Cert编码的'检查
字段为了确定
处理器是否有其中任一
此的证书类型。如果那样，
'证书颁发机构'字段是
检查为了确定是否
处理器有所有证书
那可以验证至一
指定的证明
权限。这可以是一系列
证书。

4. **CFG** - CFG_REQUEST/
CFG_REPLY允许IKE
对请求数据的终端
从其对等体。如果在的一个属性
CFG_REQUEST配置
有效负载不是零长度，它是
采取作为那的一建议
属性。CFG_REPLY
配置有效负载可能返回
该值或新的。它可以
也请添加新的属性和没有
包括一些请求部分。
申请人忽略返回
属性他们不
识别。在这些调试，
客户端请求通道
在的配置
CFG_REQUEST.ASA
回复此并且发送通道

配置属性在之后
EAP交换是成功的。

5. **SAi2** - SAI2启动SA，
哪些类似于第2阶段
在IKEv1的转换集合交换。

6. **TSi**和**Tsr** -发起者和
响应方流量选择器
包含，分别，来源
并且目的地址
发起者和响应方为了
加密的转发和接收
流量。地址范围
指定所有流量到/从
该范围被建立隧道。如果
建议是可接受对
响应方，它发送相同的TS
有效载荷上一步。

客户端必须提供为的属性
组验证在存储

AnyConnect配置文件。

***Relevant配置文件配置：**

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

ASA产生对IKE_AUTH消息的一答复并且准备验证对客户端。

ASA发送验证有效负载为了请求从客户端的用户凭证。ASA发送验证方法作为‘RSA’，因此它发送其自己的因为ASA是愿意使用扩展验证方法，在消息4安置一EAP有效负载并且延迟发送SAr2、TSi和Tsr，直到发起EAP数据包包含：

1. **代码：请求**-此代码由验证器发送给对等体。
2. **id：1** - id帮助匹配与请求的EAP答复。在这里值1，指示它是在EAP交换的第一数据包。此EAP请求
3. **长度：150** - EAP数据包的长度包括代码、id、长度和EAP数据。
4. **EAP数据**。

分段能发生，如果证书大或，如果证书链包括。发起者和响应方KE有效载荷能也包括大密钥，能也造成分

客户端回答与答复的EAP请求。

EAP数据包包含：

1. **代码：答复**-此代码由对等体发送对验证器以回应EAP请求。
2. **id：1** - id帮助匹配与请求的EAP答复。在这里值1，表明这是对ASA以前发送的请求的一答复(验证器)
3. **长度：252** - EAP数据包的长度包括代码、id、长度和EAP数据。
4. **EAP数据**。

ASA解密此答复，并且客户端说接收在上一个数据包的验证有效负载(与证书)并且接收从ASA的第一EAP请

这是ASA发送的第二请求对客户端。

EAP数据包包含：

1. **代码：请求**-此代码由验证器发送给对等体。
2. **id：2** - id帮助匹配与请求的EAP答复。在这里值2，指示它是在交换的第二数据包。此请求有'验证请
3. **长度：457** - EAP数据包的长度包括代码、id、长度和EAP数据。
4. **EAP数据**。

ENCR有效负载：

此有效负载解密，并且其内容解析作为另外的有效载荷。

客户端传送与EAP有效负载的另一IKE_AUTH发起者信息。
EAP数据包包含：

1. **代码：答复**-此代码由对等体发送对验证器以回应EAP请求。
2. **id：2** - id帮助匹配与请求的EAP答复。在这里值2，表明这是对ASA以前发送的请求的一答复(验证器)
3. **长度：420** - EAP数据包的长度包括代码、id、长度和EAP数据。
4. **EAP数据**。

ASA处理此答复。客户端请求用户回车凭证。此EAP答复有‘验证回复的‘设置验证’类型’。此数据包包含用户

ASA在交换建立第三EAP请求。

EAP数据包包含：

1. **代码：请求**-此代码由验证器发送给对等体。
2. **id：3** - id帮助匹配与请求的EAP答复。在这里值3，指示它是在交换的第三数据包。此数据包安排‘设
3. **长度：4235** - EAP数据包的长度包括代码、id、长度和EAP数据。
4. **EAP数据**。

ENCR有效负载：

此有效负载解密，并且其内容解析作为另外的有效载荷。

客户端发送有EAP有效负载的发起者数据包。

EAP数据包包含：

1. **代码：答复**-此代码由对等体发送对验证器以回应EAP请求。
2. **id：3** - id帮助匹配与请求的EAP答复。在这里值3，表明这是对ASA以前发送的请求的一答复(验证器
3. **长度：173** - EAP数据包的长度包括代码、id、长度和EAP数据。
4. **EAP数据**。

ASA处理此数据包。
EAP交换是成功的。ASA
准备派隧道群
在下一个信息包的配置，
由客户端以前请求
IDi有效负载。ASA接收
从客户端的响应数据包，
有'ack的' '设置验证'类型。这
答复确认EAP
'请完成'由传送的信息
早先ASA。

相关配置：

```
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交换当前是成功的。

EAP数据包包含：

1. **代码：成功**-此代码是发送由验证器对在完成EAP后的对等体认证方法。这表明对等体有顺利地验证对验证器。
2. **id：3** - id帮助匹配与请求的EAP答复。在这里值3，表明这是一答复以前发送的请求ASA (验证器)。第三集在交换的数据包是成功和EAP交换是成功的。
3. **长度：4** - EAP的长度数据包包括代码，id，长度和EAP数据。
4. **EAP数据。**

因为EAP交换是成功的，客户端发送有验证有效负载的IKE_AUTH发起者数据包。验证有效负载从共享密钥

当EAP验证指定或
暗示由客户端配置文件和
配置文件不包含
<IKEIdentity>元素，客户端发送
—ID_GROUP类型IDi有效负载与
已修复字符串*\$AnyConnectClient\$*。
ASA处理此消息。

相关配置：

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

ASA建立与SA、TSi和Tsr有效载荷的IKE_AUTH响应消息。

IKE_AUTH响应数据包包含：

1. **ISAKMP报头**- SPI/version/flags.
2. **验证有效负载**-使用选定的认证方法。
3. **CFG** - CFG_REQUEST/CFG_REPLY允许IKE终端对其对等体的请求数据。如果在CFG_REQUEST中包含attributes的。
4. **SAr2** - SAr2启动SA，类似于在IKEv1的第2阶段转换集合交换。
5. **TSi和Tsr** -发起者和响应方流量选择器包含，分别，发起者的源地址和目的地址和响应方为了转发和接收。

ENCR有效负载：

此有效负载解密，并且其内容解析作为另外的有效载荷。

ASA派出此IKE_AUTH响应消息，被分段到九数据包。IKE_AUTH交换完成。

连接被输入到安全关联(SA)数据库，并且状态注册。ASA也执行一些检查类似普通的访问卡(CAC)重复项S


```

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

从显示crypto sa ikev2命令的输出示例是：

```
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

```

从detail命令显示crypto的ikev2 sa的输出示例是：

```
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

从show crypto ipsec sa命令的输出示例是：

```
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
```

相关信息

- [RFC 4306，互联网密钥交换\(IKEv2\)协议](#)
- [RFC 3748，可扩展的认证协议\(EAP\)](#)
- [RFC 5996，互联网密钥交换协议版本2 \(IKEv2\)](#)
- [技术支持和文档 - Cisco Systems](#)