《ASA IPsec和IKE調試（IKEv1主動模式）故障排除技術說明》

目錄

簡介

本檔案介紹在使用主動模式和預先共用金鑰(PSK)時，思科調適型安全裝置(ASA)上的偵錯。還討論了將某些調試行轉換為配置的問題。思科建議您瞭解IPsec和網際網路金鑰交換(IKE)的基本知識。

本文不討論建立通道後傳遞的流量。

核心問題

IKE和IPsec調試有時是隱藏的，但您可以使用它們來瞭解IPsec VPN隧道建立的問題。

案例

主動模式通常用於帶有軟體（Cisco VPN客戶端）和硬體客戶端(Cisco ASA 5505自適應安全裝置或Cisco IOS？的Easy VPN(EzVPN)的情況。軟體路由器)，但僅當使用預共用金鑰時才使用。與主模式不同，主動模式包含三個消息。

調試來自運行軟體版本8.3.2並充當EzVPN伺服器的ASA。EzVPN客戶端是軟體客戶端。

使用debug指令

以下是本文中使用的debug指令：

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

ASA配置

本示例中的ASA配置應嚴格為基本；未使用外部伺服器。

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

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

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

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

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

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

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

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

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

調試

附註：使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

伺服器消息說明

從客戶端接收AM1。

處理AM1。將收到的建議和轉換與已配置的提議和轉換進行比較。
相關配置：
在介面上啟用ISAKMP，並且至少定義了一個與客戶端傳送內容匹配的策略：

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

存在與標識名稱匹配的隧道組：

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

構建AM2。此過程包括：
— 選定的策略
- Diffie-hellman(DH)
— 響應方ID
— 身份驗證
— 網路位址轉譯(NAT)偵測負載

傳送AM2。

從客戶端接收AM3。

進程AM 3.確認NAT穿越(NAT-T)的使用。兩端現在均已準備好啟動流量加密。

起始階段1.5(XAUTH)，並請求使用者認證。

接收使用者憑據。

處理使用者憑據。驗證憑據並生成模式配置負載。
相關配置：

```
username cisco
password cisco
```

傳送xuath結果。

接收並處理ACK;伺服器沒有響應。

Receive mode-config request。
Process mode-config request。 其中的許多值通常在組策略中配置。但是，由於本示例中的伺服器具有非常基本的配置，因此您在此處看不

使用配置的所有值構建模式配置響應。
相關配置：
請注意，在這種情況下，系統會始終為使用者分配相同的IP。

```
username cisco
attributes
vpn-framed-ip-
address 192.168.1.100
255.255.255.0
group-policy EZ
internal
group-policy EZ
attributes
password-storage
enabledns-server value
192.168.1.129
vpn-tunnel-protocol
ikev1
split-tunnel-policy
tunnelall
split-tunnel-network-
list value split default-
domain value
jyoungta-
labdomain.cisco.com
```

傳送模式配置響應。

階段1在伺服器上完成。啟動快速模式(QM)進程。

為客戶端構建並傳送DPD。

接收QM1。

進程QM1。

相關配置：

```
crypto dynamic-map
DYN 10 set transform-
set TRA
```

構建QM2。

相關配置：

```
tunnel-group EZ
type remote-access !
(tunnel type ra = tunnel
type remote-access)
crypto ipsec transform-
set TRA esp-aes esp-
sha-hmac
crypto ipsec security-
association lifetime
seconds 28800
crypto ipsec security-
association lifetime
kilobytes 4608000
crypto dynamic-map
```

```
DYN 10 set transform-
set TRA
crypto map MAP 65000
ipsec-isakmp dynamic
DYN
crypto map MAP
interface outside
```

傳送QM2。

接收QM3。

處理QM3。建立入站和出站安全引數索引(SPI)。 為主機新增靜態路由。

相關配置：

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

階段2完成。雙方現在都在加密和解密。
對於硬體客戶端，接收另一條消息，其中客戶端傳送有關自身的資訊。如果您仔細檢視，應找到EzVPN客

通道驗證

ISAKMP

sh cry isa sa det命令的輸出為：

```
 Active SA: 1
 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

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

IPsec

由於網際網路控制訊息通訊協定(ICMP)用於觸發通道，因此只有一個IPsec SA處於開啟狀態。通訊協定1是ICMP。請注意，SPI值與調試中協商的值不同。實際上，這是在第2階段重新生成金鑰之後的同一隧道。

sh crypto ipsec sa命令的輸出如下：

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

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

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
 #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.48.67.14/0, remote crypto endpt.: 10.48.66.23/0
 path mtu 1500, ipsec overhead 74, media mtu 1500
 current outbound spi: C4B9A77C
 current inbound spi : EA2B6B15

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

相關資訊

- [關於IPsec的維基百科文章]
- [IPsec 疑難排解：瞭解和使用偵錯指令]
- [技術支援與文件 - Cisco Systems]