疑難排解常見的 L2L 和遠端存取 IPsec VPN 問題

目錄

簡介

本文說明 IPsec VPN 問題最常見的解決方法。

背景資訊

此處所述的解決方案直接來自Cisco技術支援解決的服務請求。

其中許多解決方案是在IPsec VPN連線的深度故障排除之前實施的。

本文檔概述了在開始排除連線故障之前應嘗試執行的常見步驟。

雖然本文檔中的配置示例適用於路由器和安全裝置，但幾乎所有這些概念也適用於VPN 3000 。

有關用於在Cisco IOS® 軟體和Cisco IOS上排除IPsec問題的常見debug命令的說明，請參閱[IP安全故障排除-瞭解和使用debug](#) 命令。

注意：ASA不會透過IPSec VPN隧道傳遞組播流量。

警告：本文檔中介紹的許多解決方案都可能導致裝置上所有IPSec VPN連線暫時丟失。

建議您謹慎地實施這些解決方案，並遵循您的更改控制策略。

必要條件

需求

思科建議瞭解以下思科裝置上的IPsec VPN配置：

- Cisco ASA 5500系列安全裝置
- 思科IOS®路由器

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASA 5500系列安全裝置
- Cisco IOS®

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需更多文件慣例的相關資訊，請參閱思科技術提示慣例。

IPsec VPN配置不起作用

問題

最近配置或修改的IPSec VPN解決方案不起作用。

當前IPsec VPN配置不再有效。

解決方案

本節包含最常見IPsec VPN問題的解決方案。

儘管這些解決方案未按任何特定順序列出，但可以用作專案核對表，在您進行深入補救之前進行驗證或嘗試。

所有這些解決方案都直接來自TAC服務請求，並已解決了許多問題。

- 啟用NAT穿越(#1 RA VPN問題)
- 正確測試連線
- 啟用ISAKMP
- 啟用/停用PFS
- 清除舊的或現有的安全關聯（隧道）
- 驗證ISAKMP生存時間
- 啟用或停用ISAKMP Keepalive
- 重新輸入或恢復預共用金鑰
- 預共用金鑰不匹配
- 刪除並重新應用加密對映
- 驗證sysopt命令是否存在（僅限/ASA）

- 驗證ISAKMP身份
- 驗證空閒/會話超時
- 驗證ACL是否正確且繫結到加密對映
- 驗證ISAKMP策略
- 檢驗路由是否正確
- 驗證轉換集是否正確
- 驗證加密對映序列號和名稱
- 驗證對等體IP地址是否正確
- 驗證隧道組和組名稱
- 停用L2L對等體的XAUTH
- VPN池耗盡
- VPN客戶端流量的延遲問題

注意：由於空間方面的考慮，這些部分中的某些命令已分成兩行。

啟用NAT穿越(#1 RA VPN問題)

NAT穿越（或NAT-T）允許VPN資料流透過NAT或PAT裝置，例如Linksys SOHO路由器。

如果未啟用NAT-T，則VPN客戶端使用者通常看起來可以順利連線到ASA，但是無法訪問安全裝置後面的內部網路。

如果您未在NAT/PAT裝置中啟用NAT-T，則會在ASA中收到錯誤消息**regular translation creation failed for protocol 50 src inside : 10.0.1.26 dst outside : 10.9.69.4**。

同樣，如果無法從同一IP地址同時登入，則會顯示**Secure VPN connection terminated locally by client.原因412：遠端對等體不再響應。**出現錯誤消息。

在頭端VPN裝置中啟用NAT-T以解決此錯誤。

注意：使用Cisco IOS®軟體版本12.2(13)T及更高版本時，Cisco IOS®中預設啟用NAT-T。

以下是用於在思科安全裝置上啟用NAT-T的命令。本例中的二十(20)是保持連線時間（預設值）。

ASA

```
<#root>

securityappliance(config)#

crypto isakmp nat-traversal 20
```

使用者端也需要修改才能正常運作。

在Cisco VPN Client中，導航到Connection Entries，然後按一下Modify。它會開啟新視窗，您必須在其中選擇「傳輸」標籤。

在此頁籤下，按一下Enable Transparent Tunnelingand theIPSec over UDP (NAT / PAT)單選按鈕。然後按一下儲存並測試連線。

透過配置ACL允許NAT-T、UDP 500和ESP埠使用UDP 4500非常重要，因為ASA充當NAT裝置。

要瞭解有關ASA中ACL配置的詳細資訊，請參閱配置一條透過防火牆（執行NAT）的IPSec隧道。

正確測試連線

VPN連線最好透過執行加密的端點裝置之後的裝置進行測試，然而許多使用者在執行加密的裝置上使用ping命令測試VPN連線。

雖然ping通常可實現此目的，但使ping命令源自正確的介面非常重要。

如果ping的來源不正確，則VPN連線可能表現為已發生故障，但實際上它仍在正常工作。以下是一個示例：

路由器A加密ACL

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

路由器B加密ACL

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

在這種情況下，aping必須來源於任一個路由器之後的「內部」網路。這是因為加密ACL僅設定為加密具有那些來源位址的流量。

源自任一路由器的外部介面的連線不會加密。在特權EXEC模式下使用ping命令的擴展選項，可以使ping源自路由器的「內部」介面：

```
<#root>

routerA#

ping

Protocol [ip]:

Target IP address: 192.168.200.10
```

```
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 192.168.100.1

Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.100.1

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = ½/4 ms
```

假設此圖中的路由器已替換為ASA安全裝置。用於測試連線的Ping也可以源自具有insidekeyword的內部介面：

```
<#root>

securityappliance#

ping inside 192.168.200.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

建議不要使用yourping來定位安全裝置的內部介面。

如果必須使用yourping來定位內部介面，則必須在該介面上執行enablemanagement-accesson，否則裝置不會應答。

```
<#root>

securityappliance(config)#

management-access inside
```

當連線存在問題時，即使VPN的第一階段(1)也不起作用。

在ASA上，如果連線失敗，則SA輸出類似於以下示例，表明加密對等體配置可能錯誤和/或ISAKMP建議配置不正確：

<#root>

Router#

show crypto isakmp sa

1 IKE Peer: XX.XX.XX.XX
Type : L2L Role : initiator
Rekey : no State : MM_WAIT_MSG2

狀態可以是MM_WAIT_MSG2到MM_WAIT_MSG5，這表示主模式(MM)中相關的狀態交換失敗。

第1階段運行時的加密SA輸出類似於以下示例：

<#root>

Router#

show crypto isakmp sa

1 IKE Peer: XX.XX.XX.XX
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE

啟用ISAKMP

如果沒有指示IPSec VPN隧道正常工作，則可能是因為尚未啟用ISAKMP。請確保已在裝置上啟用ISAKMP。

使用以下命令之一在您的裝置上啟用ISAKMP：

Cisco IOS®

<#root>

router(config)#

crypto isakmp enable

Cisco ASA(用所需介面替換outsideside)

<#root>

securityappliance(config)#

crypto isakmp enable outside

在外部介面上啟用ISAKMP時，也會出現以下錯誤：

```
UDP: ERROR - socket <unknown> 62465 in used
ERROR: IkeReceiverInit, unable to bind to port
```

錯誤的原因可能是，在介面上啟用isakmp之前，ASA後面的客戶端獲得PAT到udp埠500。刪除PAT轉換(clear xlate)後，即可啟用isakmp。

驗證UDP 500和4500埠號已保留用於與對等體進行ISAKMP連線的協商。

如果在介面上未啟用ISAKMP，則VPN客戶端會顯示一條錯誤消息，類似於此消息：

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

要解決此錯誤，請在VPN網關的加密介面上啟用ISAKMP。

啟用/停用PFS

在IPsec協商中，完全正向保密(PFS)可確保每個新加密金鑰與之前的任何金鑰無關。

啟用或停用兩個隧道對等體上的PFS；否則，LAN到LAN (L2L) IPsec隧道不會在ASA/Cisco IOS®路由器中建立。

完全正向保密(PFS)是思科專有技術，第三方裝置不支援它。

ASA:

PFS預設為停用。要啟用PFS，請在組策略配置模式下使用thepfscommand和enable關鍵字。若要停用PFS，請輸入disable關鍵字。

<#root>

```
hostname(config-group-policy)#
```

pfs {enable | disable}

要從配置中刪除PFS屬性，請輸入此命令的no形式。

組策略可以從其他組策略繼承PFS的值。輸入此命令的no形式，以防止值傳輸。

<#root>

```
hostname(config-group-policy)#
no pfs
```

Cisco IOS®路由器：

要指定在此加密對映條目請求新的安全關聯時IPsec必須要求PFS，請在加密對映配置模式下使用set pfscommand。

要指定IPsec在接收新安全關聯請求時需要PFS，請在加密對映配置模式下使用set pfscommand。

要指定IPsec不得請求PFS，請使用此命令的no形式。預設情況下，不請求PFS。如果未使用此命令指定任何組，則會使用group1作為預設值。

```
set pfs [group1 | group2]
no set pfs
```

對於set pfs命令：

- group1 -指定在執行新的Diffie-Hellman交換時，IPsec必須使用768位Diffie-Hellman主模陣列。
- group2 -指定在執行新的Diffie-Hellman交換時，IPsec必須使用1024位Diffie-Hellman主模陣列。

範例：

<#root>

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#
set pfs group2
```

清除舊的或當前的安全關聯（隧道）

如果Cisco IOS®®路由器中出現此錯誤消息，則問題在於SA已過期或已清除。

遠端隧道終端裝置不知道它使用過期的SA傳送資料包（不是SA建立資料包）。

當新的SA建立後，通訊將恢復，從而啟動隧道中的相關流量以建立新的SA並重新建立隧道。

<#root>

```
%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x  has no SA
```

如果清除ISAKMP（階段I）和IPsec（階段II）安全關聯(SA)，則這是解決IPsec VPN問題最簡單、通常也最好的解決方案。

如果清除SA，則無需故障排除即可經常解決各種錯誤消息和奇怪的行為。

儘管此技術易於在任何情況下使用，但在更改或增加到當前IPsec VPN配置後，幾乎總是需要清除SA。

此外，雖然可以僅清除特定的安全關聯，但當您在裝置上全局清除SA時，可以獲得最大的好處。

一旦安全關聯被清除，就有必要透過隧道傳送流量來重新建立它們。

警告：除非您指定要清除的安全關聯，否則此處列出的命令可以清除裝置上的所有安全關聯。如果其他IPSec VPN隧道正在使用中，請謹慎繼續。

1. 清除安全關聯之前先檢視安全關聯

    a. Cisco IOS®

    <#root>

    router#

    show crypto isakmp sa

    router#

    show crypto ipsec sa

    b. Cisco ASA安全裝置

    <#root>

    securityappliance#

    show crypto isakmp sa

    securityappliance#

    show crypto ipsec sa

2. 清除安全關聯。可以按粗體顯示的形式輸入每個命令，也可以按顯示的選項輸入每個命令。

    a. Cisco IOS®

        a. ISAKMP（階段I）

<#root>

```
router#

clear crypto isakmp

 ?
  <0 - 32766>  connection id of SA
  <cr>
```

b. IPsec (階段II)

<#root>

```
router#

clear crypto sa

 ?
  counters  Reset the SA counters
  map       Clear all SAs for a given crypto map
  peer      Clear all SAs for a given crypto peer
  spi       Clear SA by SPI
  <cr>
```

b. Cisco ASA安全裝置

a. ISAKMP (階段I)

<#root>

```
securityappliance#

clear crypto isakmp sa
```

b. IPsec (階段II)

<#root>

```
security appliance#

clear crypto ipsec sa

 ?

  counters  Clear IPsec SA counters
  entry     Clear IPsec SAs by entry
  map       Clear IPsec SAs by map
  peer      Clear IPsec SA by peer
  <cr>
```

驗證ISAKMP生存時間

如果使用者經常透過L2L隧道斷開連線，則問題可能出在ISAKMP SA中配置的較短生存期。

如果在ISAKMP的生存時間內出現任何差異，您會收到%ASA-5-713092： Group = x.x.x.x， IP = x.x.x.x， Failure during phase 1 rekey attempt due to collisionerror message in /ASA。

預設值為86,400秒或24小時。一般來說，較短的生命週期可提供更安全的ISAKMP協商（最高可達某個點），但是，隨著生命週期的縮短，安全裝置可以更快地設定未來的IPsec SA。

當來自兩個對等體的兩個策略包含相同的加密、雜湊、身份驗證和Diffie-Hellman引數值，並且遠端對等體的策略指定的生存時間小於或等於比較的策略中的生存時間時，進行匹配。

如果生命週期不相同，則使用較短的生命週期（來自遠端對等體的策略）。如果未找到可接受的匹配項，則IKE拒絕協商，並且未建立IKE SA。

指定SA存留期。此示例將生命週期設定為4小時(14400秒)。預設值為86400秒（24小時）。

ASA

```
<#root>

hostname(config)#

isakmp policy 2 lifetime  14400
```

Cisco IOS®路由器

```
<#root>

R2(config)#

crypto isakmp policy 10

R2(config-isakmp)#

lifetime 86400
```

如果超過配置的最大壽命，當VPN連線終止時，您會收到此錯誤消息：

安全VPN連線被客戶端本地終止。原因426：超出最大配置生存期。

為了解決此錯誤消息，請將thelifetimevalue設定為零(0)，以將IKE安全關聯的生存時間設定為無限。VPN始終處於連線狀態，不會終止。

```
hostname(config)#isakmp policy 2 lifetime 0
```

您也可以在group-policyin中停用re-xauth以解決此問題。

啟用或停用ISAKMP Keepalive

如果配置ISAKMP Keepalive，則有助於防止偶爾丟棄的LAN到LAN或遠端訪問VPN，其中包括VPN客戶端、隧道以及在一段時間不活動後丟棄的隧道。

此功能可讓通道端點監控遠端對等點的持續存在狀態，並向該對等點報告其本身的存在狀態。

如果對等體變得無響應，端點將刪除連線。

為使ISAKMP Keepalive正常工作，兩個VPN終端都必須支援它們。

在Cisco IOS®中使用以下命令配置ISAKMP Keepalive：

```
<#root>

router(config)#

crypto isakmp keepalive 15
```

使用以下命令在ASA安全裝置上配置ISAKMP Keepalive：

用於名為10.165.205.222的隧道組的Cisco ASA

```
<#root>

securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive
   threshold 15 retry 10
```

在某些情況下，必須停用此功能以解決此問題，例如，如果VPN客戶端位於阻止DPD資料包的防火牆之後。

Cisco ASA，用於名為10.165.205.222的隧道組

停用IKE keepalive處理（預設情況下啟用）。

<#root>

```
securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive


disable
```

停用Cisco VPN Client 4.x的Keepalive

在發生問題的客戶端PC上，導航到%System Root% > Program Files > Cisco Systems >VPN Client > Profileson，以停用IKE keepalive，並在適用時編輯連線的PCF檔案。

將ForceKeepAlives=0（預設值）更改為ForceKeepAlives=1。

Keepalive是Cisco專有的，不受第三方裝置的支援。

重新輸入或恢復預共用金鑰

在許多情況下，當IPSec VPN隧道不起作用時，可歸咎於簡單的打字錯誤。例如，在安全裝置上，預共用金鑰一旦輸入就會隱藏。

這種混淆使得無法檢視金鑰是否不正確。請確保已在每個VPN端點上正確輸入了任何預共用金鑰。

重新輸入金鑰以確定金鑰正確；這是一個簡單的解決方案，有助於避免深入故障排除。

在遠端訪問VPN中，檢查是否在CiscoVPN客戶端中輸入了有效的組名稱和預共用金鑰。

如果VPN客戶端和前端裝置之間的組名或預共用金鑰不匹配，則會面臨此錯誤。

```
 1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
 The received HASH payload cannot be verified
 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
3      14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
4      14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5      14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6      14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7      14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... possibly be configured with invalid group password.
8      14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
```

```
Failed to authenticate peer (Navigator:904)
9      14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
```

警告：如果刪除與加密相關的命令，則可能會關閉一個或所有VPN隧道。在刪除與加密相關的命令之前，請謹慎使用這些命令，並參閱組織的更改控制策略。

使用以下命令，以刪除和重新輸入對等體10.0.0.1或grouppngroupin Cisco IOS®的預共用金鑰：

Cisco LAN到LAN VPN

```
<#root>

router(config)#

no crypto isakmp key secretkey
   address 10.0.0.1

router(config)#

crypto isakmp key secretkey
   address 10.0.0.1
```

Cisco Remote Access VPN

```
<#root>

router(config)#

crypto isakmp client configuration
   group vpngroup

router(config-isakmp-group)#

no key secretkey

router(config-isakmp-group)#

key secretkey
```

使用以下命令，以刪除和重新輸入/ASA安全裝置上的對等體10.0.0.1的預共用金鑰安全：

思科6.x

```
<#root>

(config)#

no isakmp key secretkey address 10.0.0.1

(config)#
```

```
isakmp key secretkey address 10.0.0.1
```

Cisco /ASA 7.x及更高版本

<#root>

```
securityappliance(config)#
```

```
tunnel-group 10.0.0.1
   ipsec-attributes
```

```
securityappliance(config-tunnel-ipsec)#
```

```
no ikev1 pre-shared-key
```

```
securityappliance(config-tunnel-ipsec)#
```

```
ikev1
```

```
pre-shared-key
   secretkey
```

預共用金鑰不匹配

VPN通道的啟動斷開。出現此問題的原因是在階段I協商期間預共用金鑰不匹配。

show crypto isakmp sacommand中的MM_WAIT_MSG_6消息指示預共用金鑰不匹配，如下例所示：

<#root>

```
ASA#
```

```
show crypto isakmp sa
```

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

1         IKE Peer: 10.7.13.20
             Type : L2L                                Role : initiator
             Rekey : no                                State :
```

```
MM_WAIT_MSG_6
```

要解決此問題，請在兩台裝置中重新輸入預共用金鑰；預共用金鑰必須是唯一且匹配的。如需詳細資訊，請參閱重新輸入或復原預先共用金鑰。

刪除並重新應用加密對映

當清除安全關聯且這無法解決IPSec VPN問題時，請刪除並重新應用相關加密對映，以解決包括間斷性丟棄VPN隧道和一些VPN站點無法啟動在內的各種問題。

警告：如果從介面刪除加密對映，則它將會關閉與該加密對映關聯的所有IPSec隧道。請謹慎地執行這些步驟，並在繼續之前考慮組織的變更控制策略。

使用以下命令可刪除和替換Cisco IOS®中的加密對映：

首先從介面中刪除加密對映。請使用crypto mapcommand的no形式。

```
<#root>

router(config-if)#

no crypto map mymap
```

繼續使用thenoform刪除整個加密對映。

```
<#root>

router(config)#

no crypto map mymap 10
```

替換對等體10.0.0.1的介面Ethernet0/0上的加密對映。以下示例顯示了最低必需加密對映配置：

```
<#root>

router(config)#

crypto map mymap 10 ipsec-isakmp

router(config-crypto-map)#

match address 101

router(config-crypto-map)#

set transform-set mySET

router(config-crypto-map)#

set peer 10.0.0.1

router(config-crypto-map)#

exit

router(config)#

interface ethernet0/0
```

```
router(config-if)#
crypto map mymap
```

使用以下命令在ASA上刪除和替換加密對映：

首先從介面中刪除加密對映。請使用crypto mapcommand的no形式。

```
<#root>
securityappliance(config)#
no crypto map mymap interface outside
```

繼續使用thenoform刪除其他加密對映命令。

```
<#root>
securityappliance(config)#
no crypto map mymap 10 match
   address 101
securityappliance(config)#
no crypto map mymap set
   transform-set mySET
securityappliance(config)#
no crypto map mymap set
   peer 10.0.0.1
```

替換對等體10.0.0.1的加密對映。以下示例顯示了最低必需加密對映配置：

```
<#root>
securityappliance(config)#
crypto map mymap 10 ipsec-isakmp
securityappliance(config)#
crypto map mymap 10
   match address 101
securityappliance(config)#
crypto map mymap 10 set
   transform-set mySET
securityappliance(config)#
crypto map mymap 10 set
```

```
   peer 10.0.0.1

securityappliance(config)#

crypto map mymap interface outside
```

如果刪除並重新應用加密對映，則當頭端的IP地址發生更改時，這也可以解決連線問題。

驗證sysopt命令是否存在（僅限ASA）

命令sysopt connection permit-ipsecandsysopt connection permit-vpnallow來自IPsec隧道的資料包及其有效負載會繞過安全裝置上的介面ACL。

如果未啟用這些命令之一，在安全裝置上終止的IPSec隧道很可能會失敗。

在安全裝置軟體版本7.0及更低版本中，此情況的相關sysopt命令issysopt connection permit-ipsec。

在安全裝置軟體版本7.1(1)及更高版本中，此情況的相關sysopt命令issysopt connection permit-vpn。

在6.x中，預設情況下停用此功能。使用/ASA 7.0(1)及更高版本時，預設情況下會啟用此功能。使用以下show命令可確定裝置上是否啟用了relevantsysoptcommand：

Cisco ASA

<#root>

```
securityappliance#

show running-config all sysopt

no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret

sysopt connection permit-vpn


!--- sysopt connection permit-vpn is enabled !--- This device is running 7.2(2)
```

使用以下命令可為您的裝置啟用correctsysoptcommand：

Cisco ASA

<#root>

```
securityappliance(config)#
sysopt connection permit-vpn
```

如果不想使用sysopt connectioncommand，請顯式允許所需的相關資料流從源到目標。

例如，在外部ACL中，從遠端裝置的遠端到本地LAN和遠端裝置的外部介面的「UDP埠500」到本地裝置的外部介面。

驗證ISAKMP身份

如果IKE協商中的IPSec VPN隧道出現故障，則故障可能是因為其對等體無法辨識其對等體的身份。

當兩個對等體使用IKE建立IPsec安全關聯時，每個對等體將其ISAKMP身份傳送給遠端對等體。

根據每個主機的ISAKMP身份設定方式，傳送其IP地址或主機名。

預設情況下，防火牆裝置的ISAKMP身份設定為IP地址。

通常，以相同的方式設定安全裝置及其對等體的標識，以避免IKE協商失敗。

要對傳送至對等體的階段2 ID進行設定，請在全局配置模式下使用theisakmp identitycommand。

```
crypto isakmp identity address
!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with pre-shared key as authentication typ
```

或

```
crypto isakmp identity auto
!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by connection typ
```

或

```
crypto isakmp identity hostname
!--- Uses the fully-qualified domain name of !--- the host exchange ISAKMP identity information (defaul
```

使用ASA配置遷移工具將配置從ASA轉移到ASA後，VPN隧道無法啟動；這些消息顯示在日誌中：

[IKEv1]：組= x.x.x.x，IP = x.x.x.x，發現過時的PeerTblEntry，正在刪除！

[IKEv1]：組= x.x.x.x，IP = x.x.x.x，從相關器表中刪除對等體失敗，不匹配！

[IKEv1]：組= x.x.x.x，IP = x.x.x.x，construct_ipsec_delete()：無SPI以標識第2階段SA！

[IKEv1]：組= x.x.x.x，IP = x.x.x.x，從相關器表中刪除對等體失敗，不匹配！

驗證空閒/會話超時

如果空閒超時設定為30分鐘（預設值），則意味著在30分鐘後隧道沒有流量通過。

VPN Client將在30分鐘後斷開連線，而不管空閒超時引數如何，並且將出現**PEER_DELETE-IKE_DELETE**_UNSPECIFIED錯誤。

配置timeoutandsession timeoutasnonein使隧道變為alwaysup，並且讓隧道即使在使用第三方裝置時也不會被丟棄。

ASA

在組策略配置模式下或使用者名稱配置模式下輸入vpn-idle-timeoutcommand，以配置使用者超時時長：

<#root>

```
hostname(config)#
group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#
vpn-idle-timeout none
```

在組策略配置模式下或使用者名稱配置模式下使用vpn-session-timeoutcommand配置VPN連線的最長時間：

<#root>

```
hostname(config)#
group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#
vpn-session-timeout none
```

當配置了tunnel-all時，不需要配置configureidle-timeouting，因為即使您配置VPN-idle timeout，它

也不起作用，因為所有流量都透過隧道（因為配置了tunnel-all）。

因此，相關流量（甚至PC生成的流量）是相關的，不會讓空閒超時生效。

Cisco IOS®路由器

在全局配置模式或加密對映配置模式下，使用crypto ipsec security-association idle-timecommand以配置IPsec SA空閒計時器。

預設情況下，停用IPsec SA空閒計時器。

<#root>

crypto ipsec security-association idle-time

seconds

時間以秒為單位，空閒計時器允許非活動對等體維持SA。seconds引數的有效值範圍為60至86400。

驗證ACL是否正確且繫結到加密對映

在典型IPSec VPN配置中使用兩個訪問清單。一個訪問清單用於將發往VPN隧道的流量從NAT進程中排除。

另一個訪問清單定義要加密的流量；這包括在LAN到LAN設定中的加密ACL或遠端訪問配置中的分割隧道ACL。

當這些ACL配置錯誤或丟失時，流量可能以一個方向流過VPN隧道，或者根本不會透過隧道傳送。

確保在全局配置模式下使用crypto map match address命令將加密ACL與加密對映繫結。

請確保已配置完成IPSec VPN配置所需的所有訪問清單，並且這些訪問清單定義了正確的流量。

此清單包含當您懷疑ACL是IPSec VPN問題的原因時要檢查的簡單事項。

確保您的NAT免除和加密ACL指定了正確的流量。

如果您有多個VPN隧道和多個加密ACL，請確保這些ACL不會重疊。

確保您的裝置配置為使用NAT免除ACL。在路由器上，這意味著您使用theroute-mapcommand。

在ASA上，這意味著您使用thenat (0)命令。LAN到LAN配置和遠端訪問配置均需要NAT免除ACL。

此處，Cisco IOS®路由器配置為免除來自NAT在192.168.100.0 /24和192.168.200.0 /24或192.168.1.0 /24之間傳送的流量。發往其他任何地方的流量會受到NAT過載的影響：

```
access-list 110 deny ip 192.168.100.0 0.0.0.255
```

```
   192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any

route-map nonat permit 10
  match ip address 110

ip nat inside source route-map nonat interface FastEthernet0/0 overload
```

NAT免除ACL僅適用於IP地址或IP網路，如上述示例(access-list noNAT)，並且必須與加密對映ACL相同。

NAT免除ACL不能與埠號一起使用（例如，23、25、...）。

在VOIP環境中，網路之間的語音呼叫是透過VPN進行通訊的，如果NAT 0 ACL配置不正確，則語音呼叫將無法正常工作。

在排除故障之前，建議檢查VPN連線狀態，因為問題可能出在NAT免除ACL配置錯誤。

如果NAT免除(nat 0) ACL中有錯誤配置，您會收到如圖所示的錯誤消息。

```
%ASA-3-305005: No translation group found for
udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p
```

不正確的範例：

<#root>

```
access-list noNAT extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
```

eq 25

如果NAT免除(nat 0)不起作用，請嘗試將其刪除並發出NAT 0命令以使其正常工作。

確保您的ACL不是向後的，並且型別正確。

LAN到LAN配置的加密和NAT免除ACL必須從配置ACL的裝置的角度編寫。

這表示ACL必須能夠相互傳達。在以下示例中，在192.168.100.0 /24和192.168.200.0 /24之間建立了LAN到LAN隧道。

路由器A加密ACL

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
```

```
   192.168.200.0 0.0.0.255
```

路由器B加密ACL

```
access-list 110 permit ip 192.168.200.0 0.0.0.255
   192.168.100.0 0.0.0.255
```

雖然此處未作說明，但此概念同樣適用於ASA安全裝置。

在ASA中，遠端訪問配置的分割隧道ACL必須成為允許流量流入VPN Client需要訪問的網路的訪問清單。

Cisco IOS®路由器可以使用擴展ACL來分割隧道。在擴展訪問清單中，在分割隧道ACL中的源使用「any」相當於停用分割隧道。

請僅將擴展ACL中的源網路用於分割隧道。

正確範例：

<#root>

access-list 140 permit ip

10.1.0.0 0.0.255.255

10.18.0.0 0.0.255.255

不正確的範例：

<#root>

access-list 140 permit ip

any

10.18.0.0 0.0.255.255

Cisco IOS®

<#root>

router(config)#

access-list 10 permit ip 192.168.100.0

router(config)#

```
crypto isakmp client configuration group MYGROUP

router(config-isakmp-group)#

acl 10
```

Cisco ASA

<#root>

```
securityappliance(config)#

access-list 10 standard
   permit 192.168.100.0 255.255.255.0

securityappliance(config)#

group-policy MYPOLICY internal

securityappliance(config)#

group-policy MYPOLICY attributes

securityappliance(config-group-policy)#

split-tunnel-policy
   tunnelspecified

securityappliance(config-group-policy)#

split-tunnel-network-list
   value 10
```

站點到站點VPN隧道的ASA版本8.3中的NAT免除配置：

必須在具有版本8.3的兩台ASA的ASA和BOASA之間建立站點到站點VPN。HOASA上的NAT免除配置類似於以下內容：

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

驗證ISAKMP策略

如果IPSec隧道未啟動，請檢查ISAKMP策略是否與遠端對等體匹配。此ISAKMP策略適用於站點到站點(L2L)和遠端訪問IPsec VPN。

如果Cisco VPN Client或站點到站點VPN無法與遠端裝置建立隧道，請檢查兩個對等體是否包含相同的加密、雜湊、身份驗證和Diffie-Hellman引數值。

驗證遠端對等體策略何時指定了生存時間小於或等於發起方傳送的策略中的生存時間。

如果生命週期不相同，安全裝置將使用較短的生命週期。如果不存在可接受的匹配，ISAKMP將拒絕協商，並且不會建立SA。

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table
failed, no match!"
```

以下是詳細的日誌訊息：

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, drop
```

此消息通常是由於不匹配的ISAKMP策略或遺漏的NAT 0語句而出現的。

此外，系統還會顯示以下消息：

```
Error Message    %ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
P1 SA is complete.
```

此消息表明第1階段完成後，第2階段消息在隊列中。此錯誤消息是由以下原因之一導致的：

- 任何對等體上的階段不匹配
- ACL阻止對等體完成第1階段

此消息通常緊跟**Removing peer from peer table failed, no match!**錯誤消息。

如果Cisco VPN Client無法連線頭端裝置，則問題可能是ISAKMP策略不匹配。前端裝置必須與Cisco VPN客戶端的其中一個IKE建議匹配。

對於ASA上使用的ISAKMP策略和IPSec轉換集，Cisco VPN客戶端不能將策略與DES和SHA的組合一起使用。

如果使用DES，則需要將MD5用於雜湊演算法，或者可以使用其他組合，3DES與SHA和3DES與MD5。

檢驗路由是否正確

請確保您的加密裝置（例如路由器和ASA安全裝置）具有適當的路由資訊，以便透過VPN隧道傳送流量。

如果網關裝置後面還有其他路由器，請確保這些路由器知道如何到達隧道以及另一端的網路。

在VPN部署中，路由的一個關鍵元件是反向路由注入(RRI)。

RRI將遠端網路或VPN客戶端的動態條目放置在VPN網關的路由表中。

這些路由對安裝它們的裝置以及網路中的其他裝置都很有用，因為RRI安裝的路由可以透過路由協定（如EIGRP或OSPF）重分配。

在LAN到LAN配置中，每個端點必須擁有通往其應為其加密流量的網路的路由。

在本例中，路由器A必須包含透過10.89.129.2連線到路由器B之後的網路的路由。路由器B必須包含連線到192.168.100.0 /24的類似路由：

確保每台路由器知道相應路由的第一種方法是為每個目的網路配置靜態路由。例如，路由器A可以配置以下路由語句：

```
ip route 0.0.0.0 0.0.0.0 172.22.1.1
ip route 192.168.200.0 255.255.255.0 10.89.129.2
ip route 192.168.210.0 255.255.255.0 10.89.129.2
ip route 192.168.220.0 255.255.255.0 10.89.129.2
ip route 192.168.230.0 255.255.255.0 10.89.129.2
```

如果路由器A替換為ASA，則配置可能如下所示：

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
```

如果每個端點後面存在大量網路，則靜態路由配置將變得難以維護。

相反，建議您使用反向路由注入，如所述。RRI將加密ACL中列出的所有遠端網路的路由放入路由表中。

例如，路由器A的加密ACL和加密對映可能如下所示：

<#root>

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.210.0 0.0.0.255
```

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.220.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.230.0 0.0.0.255

crypto map myMAP 10 ipsec-isakmp
 set peer 10.89.129.2
```

reverse-route

```
 set transform-set mySET
 match address 110
```

如果路由器A被ah ASA替換，則配置可能如下所示：

<#root>

```
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.230.0 255.255.255.0

crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET
```

crypto map mymap 10 set reverse-route

在遠端訪問配置中，並不總是需要更改路由。

但是，如果VPN網關路由器或安全裝置後面還有其他路由器，這些路由器需要以某種方式獲知到VPN客戶端的路徑。

在以下示例中，假設VPN Client在連線時的給定地址在10.0.0.0 /24範圍內。

如果網關和其他路由器之間未使用路由協定，則可以在路由器（例如Router 2）上使用靜態路由：

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

如果網關和其他路由器之間使用路由協定（如EIGRP或OSPF），則建議按照說明使用反向路由注入。

RRI會自動將VPN客戶端的路由增加到網關的路由表中。然後，這些路由可以分發到網路中的其他路由器。

Cisco IOS®路由器：

<#root>

```
crypto dynamic-map dynMAP 10
 set transform-set mySET
```

reverse-route

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Cisco ASA安全裝置：

<#root>

```
crypto dynamic-map dynMAP 10 set transform-set mySET
```

crypto dynamic-map dynMAP 10 set reverse-route

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

如果為VPN客戶端分配的IP地址池與前端裝置的內部網路重疊，則會出現路由問題。有關詳細資訊，請參閱專用網路重疊部分。

驗證轉換集是否正確

確保兩端轉換集要使用的IPsec加密和雜湊演算法相同。

有關詳細資訊，請參閱Cisco安全裝置配置指南的命令參考。

對於ASA上使用的ISAKMP策略和IPSec轉換集，Cisco VPN客戶端不能將策略與DES和SHA的組合一起使用。

如果使用DES，則需要將MD5用於雜湊演算法，或者可以使用其他組合，3DES與SHA和3DES與MD5。

驗證加密對映序列號和名稱以及在IPSec隧道啟動/結束時加密對映是否應用到正確的介面

如果在同一加密對映上配置了靜態和動態對等體，則加密對映條目的順序非常重要。

動態加密對映entrymust的序列號必須高於其他所有靜態加密對映條目。

如果靜態條目的編號高於動態條目，則與這些對等體的連線會失敗，並顯示如圖所示的調試。

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600011)!
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

安全裝置中的每個介面只允許有一個動態加密對映。

以下是包含靜態條目和動態條目的正確編號加密對映示例。請注意，動態條目的序列號最高，並且留有空間以增加其他靜態條目：

<#root>

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
```

crypto map mymap 60000 ipsec-isakmp dynamic ciscothe

加密對映名稱區分大小寫。

當動態加密人序列不正確導致對等體命中錯誤的加密對映時，也會出現此錯誤消息。

這也由定義相關流量的加密訪問清單不匹配導致：**%ASA-3-713042： IKE發起程式無法找到策略：**

如果要在同一介面中終止多個VPN隧道，請建立具有相同名稱（每個介面只允許一個加密對映）但序列號不同的加密對映。

對於路由器和ASA也是如此。

同樣，有關L2L和遠端訪問VPN方案的加密對映配置的詳細資訊，請參閱ASA：向現有L2L VPN增加新隧道或遠端訪問-Ciscoin。

驗證對等體IP地址是否正確

建立和管理IPsec的連線特定記錄的資料庫。

對於ASA安全裝置LAN到LAN (L2L) IPsec VPN配置，請在tunnel-group <name> type ipsec-l2lcommand中將隧道組的<name>指定為遠端對等體IP地址（遠端隧道端）。

對等體IP地址必須與intunnel group name和Crypto map set addresscommands匹配。

當您使用ASDM配置VPN時，它自動生成了隧道組名稱以及正確的對等IP地址。

如果未正確配置對等體IP地址，則日誌中會包含以下消息，可以透過正確配置對等體IP地址來解決該問題。

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

當在ASA加密配置中未正確配置對等體IP地址時，ASA無法建立VPN隧道，並且僅在MM_WAIT_MSG4階段掛起。

要解決此問題，請更正配置中的對等體IP地址。

以下是VPN隧道在MM_WAIT_MSG4狀態掛起時，show crypto isakmp命令的輸出結果。

<#root>

```
hostname#
show crypto isakmp sa

1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG4
```

驗證隧道組和組名稱

```
%ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy
```

當由於組策略中指定的允許隧道與隧道組配置中的允許隧道不同而丟棄隧道時，會出現此消息。

<#root>

```
group-policy hf_group_policy attributes
  vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
  vpn-tunnel-protocol l2tp-ipsec
```

Both lines read:

```
  vpn-tunnel-protocol ipsec l2tp-ipsec
```

對預設組策略中已存在的協定啟用預設組策略中的IPSec。

```
group-policy DfltGrpPolicy attributes
   vpn-tunnel-protocol L2TP-IPSec IPSec webvpn
```

停用L2L對等體的XAUTH

如果LAN到LAN隧道和遠端訪問VPN隧道配置在同一個加密對映中，則系統會對LAN到LAN對等體提示XAUTH資訊，且LAN到LAN隧道出現故障，在how crypto isakmp sacommand的輸出中顯示「CONF_XAUTH」。

以下是SA輸出的示例：

<#root>

```
Router#
```

```
show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot  status
X.X.X.X         Y.Y.Y.Y         CONF_XAUTH       10223    0   ACTIVE
X.X.X.X         Z.Z.Z.Z         CONF_XAUTH       10197    0   ACTIVE
```

此問題僅適用於Cisco IOS®，而ASA則不受此問題影響，因為它使用隧道組。

請在輸入isakmp金鑰時使用o-xauthkeyword，以便裝置不會提示對等體提供XAUTH資訊（使用者名稱和口令）。

此關鍵字停用靜態IPsec對等體的XAUTH。在相同加密對映上配置了L2L和RA VPN的裝置上輸入類似如下所示的命令：

<#root>

```
router(config)#
```

```
crypto isakmp key cisco123 address
   172.22.1.164 no-xauth
```

在ASA充當Easy VPN伺服器的情況下，Easy VPN客戶端由於Xauth問題而無法連線到頭端。

在ASA中停用使用者身份驗證以解決問題，如下所示：

<#root>

```
ASA(config)#
```

```
tunnel-group example-group type ipsec-ra
```

```
ASA(config)#
```

```
tunnel-group example-group ipsec-attributes
```

```
ASA(config-tunnel-ipsec)#
```

```
isakmp ikev1-user-authentication none
```

請參閱本文檔的Miscellaneoussection，以瞭解有關theisakmp ikev1-user-authenticationcommand的詳細資訊。

VPN池耗盡

當分配給VPN池的IP地址範圍不足時，可以透過兩種方式擴展IP地址的可用性：

1. 移除現有範圍，然後定義新範圍。以下是範例：

```
<#root>
CiscoASA(config)#
no ip local pool testvpnpool 10.76.41.1-10.76.41.254
CiscoASA(config)#
ip local pool testvpnpool 10.76.41.1-10.76.42.254
```

2. 當不連續子網增加到VPN池時，您可以定義兩個獨立的VPN池，然後按照「隧道組屬性」下的順序進行指定。以下是範例：

```
<#root>
CiscoASA(config)#
ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254
CiscoASA(config)#
ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254
CiscoASA(config)#
tunnel-group test type remote-access
CiscoASA(config)#
tunnel-group test general-attributes
CiscoASA(config-tunnel-general)#
address-pool (inside) testvpnpoolAB testvpnpoolCD
CiscoASA(config-tunnel-general)#
exit
```

您指定池的順序非常重要，因為ASA按照池在此命令中的顯示順序分配來自這些池的地址。

group-policy address-pools命令中的address-pools設定始終覆蓋tunnel-group address-pool命令中的本地池設定。

VPN客戶端流量的延遲問題

當VPN連線存在延遲問題時，請驗證以下條件以解決此問題：

1. 驗證是否可以進一步降低封包的MSS。
2. 如果使用的是IPsec/tcp而不是IPsec/udp，則配置represerve-vpn-flow。
3. 重新載入Cisco ASA。

VPN客戶端無法與ASA連線

問題

當X-auth用於RADIUS伺服器時，Cisco VPN Client無法進行身份驗證。

解決方案

問題可能是xauth超時。增加AAA伺服器的超時值以解決此問題。

舉例來說：

<#root>

```
Hostname(config)#
aaa-server test protocol radius

hostname(config-aaa-server-group)#
aaa-server test host 10.2.3.4

hostname(config-aaa-server-host)#
timeout 10
```

問題

當X-auth用於RADIUS伺服器時，Cisco VPN Client無法進行身份驗證。

解決方案

最初，請確保身份驗證工作正常。要縮小問題範圍，首先使用ASA上的本地資料庫驗證身份驗證。

```
tunnel-group tggroup general-attributes
              authentication-server-group none
              authentication-server-group LOCAL
```

```
exit
```

如果這樣可以正常工作，則問題與Radius伺服器配置有關。

從ASA驗證RADIUS伺服器的連線。如果ping操作沒有出現任何問題，請檢查ASA上的RADIUS相關配置和RADIUS伺服器上的資料庫配置。

您可使用debug radiuscommand對Radius相關問題進行故障排除。有關sampledebug radiusoutput的資訊，請參閱thisSample Output。

在ASA上使用debugcommand之前，請參閱以下文檔：警告消息。

VPN客戶端在第一次嘗試時經常丟棄連線或「Security VPN Connection terminated by peer.Reason 433.」或「Secure VPN Connection terminated by Peer Reason 433：(Reason Not Specified by Peer)」

問題

Cisco VPN客戶端使用者在嘗試與頭端VPN裝置連線時收到此錯誤。

VPN客戶端在第一次嘗試時經常丟棄連線

安全VPN連線由對等體終止。理由433.

安全VPN連線被對等體原因433終止：（對等體未指定原因）

嘗試分配網路或廣播IP地址，從池中刪除(x.x.x.x)

解決方案1

問題可能是透過ASA、Radius伺服器、DHCP伺服器或充當DHCP伺服器的Radius伺服器來分配IP池。

請使用debug cryptocommand，以驗證網路掩碼和IP地址是否正確。此外，請驗證地址池中不包含網路地址和廣播地址。

Radius伺服器必須能夠為使用者端指派正確的IP位址。

解決方案2

由於擴展身份驗證失敗，也會出現此問題。必須檢查AAA伺服器才能對此錯誤進行故障排除。

檢查伺服器和使用者端上的伺服器驗證密碼。重新載入AAA伺服器可以解決此問題。

解決方案3

此問題的另一個解決方法是停用威脅檢測功能。

當針對不同不完整安全關聯(SA)進行多次重新傳輸時，啟用威脅檢測功能的ASA會認為發生了掃描攻擊，並且VPN埠被標籤為主威脅。

嘗試停用威脅檢測功能，因為這會導致ASA處理產生大量開銷。使用以下命令以停用威脅偵測：

```
no threat-detection basic-threat
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

這可以當作一種解決方法，以驗證這是否修正了實際的問題。

確保在Cisco ASA上停用威脅檢測實際上會破壞幾項安全功能，例如減少掃描嘗試、無效SPI的DoS、應用檢查失敗的資料包以及不完整的會話。

解決方案4

當轉換集配置不正確時，也會出現此問題。正確配置轉換集可解決此問題。

遠端訪問和EZVPN使用者連線到VPN，但無法訪問外部資源

問題

遠端訪問使用者連線到VPN後即無法連線Internet。

遠端訪問使用者無法訪問位於同一裝置上其他VPN後面的資源。

遠端訪問使用者只能訪問本地網路。

解決方案

請嘗試以下解決方案以解決此問題：

- 無法訪問DMZ中的伺服器
- VPN客戶端無法解析DNS
- 分割隧道-無法訪問Internet或排除的網路
- 本地LAN訪問
- 專用網路重疊

無法訪問DMZ中的伺服器

一旦使用VPN前端裝置(ASA/Cisco IOS®路由器)建立了IPsec隧道，VPN客戶端使用者就可以訪問內部網路(10.10.10.0/24)資源，但是無法訪問DMZ網路(10.1.1.0/24)。

圖表

檢查是否已在頭端裝置中增加Split Tunnel， NO NAT配置，以訪問DMZ網路中的資源。

範例：

ASA配置：

此配置顯示如何配置DMZ網路的NAT免除，以便使VPN使用者能夠訪問DMZ網路：

```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

為NAT配置增加新條目後，清除NAT轉換。

```
Clear xlate
Clear local
```

驗證:

如果已建立隧道，請轉到Cisco VPN客戶端並選擇Status > Route詳細資訊，以檢查是否已顯示DMZ和內部網路的安全路由。

有關將新VPN隧道或遠端訪問VPN增加到已經存在的L2L VPN配置所需的步驟，請參閱ASA：向現有L2L VPN增加新隧道或遠端訪問VPN - Cisco。

有關在透過隧道連線到Cisco 5500系列自適應安全裝置(ASA)時如何允許VPN Client訪問Internet的分步說明，請參閱ASA：在ASA上允許VPN Client使用分割隧道配置示例。

VPN客戶端無法解析DNS

隧道建立後，如果VPN客戶端無法解析DNS，問題可能是頭端裝置(ASA)中的DNS伺服器配置。

還要檢查VPN客戶端和DNS伺服器之間的連線。DNS伺服器配置必須在組策略下配置，並在隧道組常規屬性中的組策略下應用；例如：

```
<#root>
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1) !--- a
```

```
group-policy vpn3000 internal
group-policy vpn3000 attributes
 dns-server value 172.16.1.1
 default-domain value cisco.com


!--- Associate the group policy(vpn3000) to the tunnel group !--- with the default-group-policy.


tunnel-group vpn3000 general-attributes
 default-group-policy vpn3000
```

VPN Client無法按名稱連線內部伺服器

VPN客戶端無法按名稱ping遠端或頭端內部網路的主機或伺服器。您需要在ASA上啟用分割DNS配置，以便解決此問題。

分割隧道-無法訪問Internet或排除的網路

分割通道讓遠端存取IPsec使用者端有條件地將封包以加密形式透過IPsec通道導向或以明文形式導向網路介面（以解密形式傳送），然後傳送到最終目的地。

預設情況下，分割隧道處於停用狀態，這會顯示unnelalltraffic。

```
split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}
```

僅Cisco VPN Client支援excludespecified選項，EZVPN Client不支援該選項。

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

有關分割隧道的詳細配置示例，請參閱以下文檔：

- ASA：在ASA上允許VPN客戶端使用分割隧道的配置示例
- 路由器允許VPN Client使用分割隧道連線IPsec和Internet的配置示例

髮夾溶液

此功能對於進入介面然後從同一介面路由出去的VPN流量很有用。

例如，在中心輻射型VPN網路中，安全裝置是中心網路，遠端VPN網路是輻射型，輻射到輻射型通訊流量必須進入安全裝置，然後再次流出到另一個輻射型。

使用same-security-trafficconfiguration以允許資料流進入和退出同一介面。

```
<#root>

securityappliance(config)#

same-security-traffic permit intra-interface
```

本地LAN訪問

遠端訪問使用者連線到VPN，並且只能連線到本地網路。

有關詳細配置示例，請參閱ASA：允許VPN Client的本地LAN訪問。

專用網路重疊

問題

如果在建立隧道後無法訪問內部網路，請檢查分配給與前端裝置後方的內部網路重疊的VPN客戶端的IP地址。

解決方案

驗證池中要分配給VPN客戶端的IP地址、前端裝置的內部網路以及VPN客戶端內部網路是否位於不同的網路中。

您可以為同一個主網路分配不同的子網，但有時會出現路由問題。

有關更多示例，請參閱無法訪問DMZ中的伺服器DiagramandExamplel部分。

無法連線超過三個VPN客戶端使用者

問題

只有三個VPN客戶端可以連線到ASA/；第四個客戶端的連線失敗。失敗時，會顯示此錯誤訊息：

```
Secure VPN Connection terminated locally by the client.
     Reason 413: User Authentication failed.
```

```
tunnel rejected; the maximum tunnel count has been reached
```

解決方案

在大多數情況下，此問題與組策略中的同時登入設定和最大會話限制有關。

請嘗試以下解決方案以解決此問題：

- 設定同時登入
- 使用CLI配置ASA
- 配置配置

設定同時登入

如果選中了ASDM中的Inheritcheck框，則系統僅允許預設的使用者同時登入數。同時登入的預設值是三(3)。

為了解決此問題，請增加同時登入的值。

1. 啟動ASDM，然後導航到Configuration > VPN > Group Policy。
2. 選擇適當的群組，然後按一下「編輯」按鈕。
3. 進入Generaltab後，撤消連線設定下的Simultaneous LoginsunderConnection的Inheritcheck框。在欄位中選擇適當的值。

   此欄位的最小值為零(0)，這將停用登入並阻止使用者訪問。

   當您使用同一使用者帳戶從另一台PC登入時，當前會話（從另一台使用同一使用者帳戶的PC建立的連線）將終止，並會建立新會話。

這是預設行為，獨立於VPN同時登入。

使用CLI配置ASA

完成以下步驟以配置所需的同時登入數。在本例中，選擇二十(20)作為期望值。

```
<#root>

ciscoasa(config)#

group-policy Bryan attributes

ciscoasa(config-group-policy)#

vpn-simultaneous-logins 20
```

要瞭解有關此命令的詳細資訊，請參閱Cisco安全裝置命令參考。

在全局配置模式下使用vpn-sessiondb max-session-limitcommand，將VPN會話數限制為小於安全裝置允許的值。

使用此命令的版本以刪除會話限制。請再次使用此命令，覆寫目前的設定。

```
vpn-sessiondb max-session-limit {session-limit}
```

此示例顯示如何將VPN會話最大限制設定為450：

```
<#root>

hostname#

vpn-sessiondb max-session-limit 450
```

設定

錯誤消息

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

解決方案

完成以下步驟以配置所需的同時登入數。您也可以嘗試將此SA的「同時登入」設定為5：

選擇Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneous Logins，然後將登入數更改為5。

建立通道後無法啟動工作階段或應用程式，且傳輸緩慢

問題

建立IPSec通道後，應用程式或作業階段不會透過通道啟動。

解決方案

使用ping命令，以檢查網路或檢視是否可從您的網路訪問應用程式伺服器。

對於透過路由器或/ASA裝置的臨時資料包（特別是已設定SYN位的TCP資料段），這可能是一個最大資料段大小(MSS)問題。

Cisco IOS®路由器-更改路由器的外部介面（隧道終端介面）中的MSS值

執行下列命令，以變更路由器外部介面（通道結束介面）中的MSS值：

```
<#root>

Router>

enable

Router#

configure terminal

Router(config)#

interface ethernet0/1


Router(config-if)#ip tcp adjust-mss 1300

Router(config-if)#

end
```

以下訊息顯示TCP MSS的偵錯輸出：

```
<#root>

Router#debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 1300, MSS is
1300
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

在路由器上，MSS會根據配置調整為1300。

有關詳細資訊，請參閱ASA和Cisco IOS®：VPN分段。

ASA -請參閱/ASA文檔

無法正確訪問Internet或透過隧道傳輸緩慢，因為它會出現MTU大小錯誤消息和MSS問題。

若要解決此問題，請參閱以下檔案：

- ASA和Cisco IOS®：VPN分段

無法從ASA啟動VPN隧道

問題

您無法從ASA介面啟動VPN隧道，並且建立隧道後，遠端端/VPN客戶端無法ping通VPN隧道上ASA的內部介面。

例如，pn客戶端無法通過VPN隧道啟動到ASA內部介面的SSH或HTTP連線。

解決方案

除非在全局配置模式下配置management-accesscommand，否則無法從隧道的另一端對的內部介面執行ping操作。

```
<#root>

ASA-02(config)#

management-access inside


ASA-02(config)#

show management-access

management-access inside
```

此命令還可幫助透過VPN隧道建立到ASA內部介面的ssh初始化或http連線。

此資訊對DMZ介面同樣適用。例如，如果您想要對/ASA的DMZ介面執行ping操作或想要從DMZ介面啟動隧道，則需要使用management-access DMZ命令。

```
<#root>

ASA-02(config)#

management-access DMZ
```

如果VPN客戶端無法連線，請確保ESP和UDP埠打開。

但是，如果這些埠未打開，請嘗試在TCP 10000上連線，並在VPN客戶端連線條目下選擇此埠。

按一下右鍵modify > transport頁籤> IPsec over TCP。

無法通過VPN隧道傳遞流量

問題

您無法通過VPN隧道傳遞流量。

解決方案

當ESP資料包被阻止時，也會出現此問題。要解決此問題，請重新配置VPN隧道。

當資料未加密，但僅透過VPN隧道解密時，可能會發生此問題，如以下輸出所示：

<#root>

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
    Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
      access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
      local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
      current_peer: y.y.y.y


 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 393, #pkts decrypt: 393, #pkts verify: 393

      #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: 0
```

要解決此問題，請檢查以下條件：

1. 如果加密訪問清單與遠端站點匹配，並且NAT 0訪問清單正確。
2. 如果路由正確，且流量確實到達透過內部的外部介面。示例輸出顯示解密已完成，但不會進行加密。
3. 如果已在ASA上配置了sopt permit connection-vpn命令。如果未配置，請配置此命令，因為它允許ASA從介面ACL檢查中排除加密/VPN流量。

為同一加密對映上的VPN隧道配置備用對等體

問題

您想為單個VPN隧道使用多個備份對等體。

解決方案

配置多個對等體相當於提供備用清單。對於每個隧道，安全裝置會嘗試與清單中的第一個對等體協商。

如果該對等裝置不響應，安全裝置將沿清單向下依次工作，直到對等裝置響應或者清單中不再有對等裝置。

ASA已將加密對映配置為主對等體。可以在主要對等體之後增加輔助對等體。

此示例配置將主對等體顯示為X.X.X.X，將備份對等體顯示為Y.Y.Y.Y：

<#root>

ASA(config)#

crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y

停用/重新啟動VPN隧道

問題

要臨時停用VPN隧道並重新啟動服務，請完成本節中介紹的過程。

解決方案

在全局配置模式下使用crypto map interface命令可刪除之前在介面上定義的加密對映集。

使用此命令的thenoform，從介面中刪除加密對映集。

<#root>

hostname(config)#

no crypto map

map-name

interface

interface-name

此命令將刪除到任何活動安全裝置介面的加密對映集，並使IPSec VPN隧道在該介面處於非活動狀態。

要重新啟動介面上的IPSec隧道，您必須先將加密對映集分配給介面，然後該介面才能提供IPSec服務。

<#root>

hostname(config)#

crypto map

map-name

interface

interface-name

部分通道未加密

問題

當VPN網關上配置了大量隧道時，某些隧道不會傳遞流量。ASA不會接收這些隧道的加密資料包。

解決方案

出現此問題的原因是ASA無法通過隧道傳遞加密資料包。在ASP表中建立了重複的加密規則。

錯誤：- %ASA-5-713904：組= DefaultRAGroup，IP = x.x.x.x，...不支援的事務模式v2版本。隧道已終止。

問題

顯示**%ASA-5-713904： Group = DefaultRAGroup， IP = 192.0.2.0，...unsupported Transaction Mode v2 version.Tunnel**錯誤消息。

解決方案

Transaction Mode v2錯誤消息的原因是ASA僅支援IKE模式配置V6而不支援舊版V2模式。

請使用IKE模式配置V6版本解決此錯誤。

錯誤：- %ASA-6-722036：組客戶端組使用者xxxx IP x.x.x.x傳輸大資料包1220（閾值1206）

問題

ASA的日誌中顯示**%ASA-6-722036： Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206)**錯誤消息。

此日誌意味著什麼？如何解決此問題？

解決方案

此日誌消息表明向客戶端傳送了一個大型資料包。封包的來源不知道使用者端的MTU。

這也可能是因為壓縮了不可壓縮的資料。解決方法是使用svc compression nonecommand關閉SVC壓縮，即可解決問題。

在VPN隧道一端啟用QoS時出現錯誤消息

問題

如果在VPN隧道的一端啟用了QoS，則會收到以下錯誤消息：

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay check
```

解決方案

此消息通常在隧道的一端執行QoS時出現。當檢測到資料包順序混亂時，會出現這種情況。

您可以停用QoS以停止此功能，但只要流量能夠透過隧道，就可以忽略此功能。

警告：加密對映條目不完整

問題

當您運行crypto map mymap 20 ipsec-isakmpcommand時，您會收到以下錯誤：

警告：加密對映條目不完整

舉例來說：

<#root>

```
ciscoasa(config)#
crypto map mymap 20 ipsec-isakmp
WARNING: crypto map entry incomplete
```

解決方案

這是定義新加密對映時的常見警告；提醒必須在配置訪問清單（匹配地址）、轉換集和對等體地址等引數後才能生效。

為定義加密對映而鍵入的第一行沒有在配置中顯示也是正常的。

錯誤：- %ASA-4-400024： IDS：2151 Large ICMP packet from to on interface outside

問題

無法通過vpn隧道傳遞大型ping資料包。當我們嘗試傳遞大型ping資料包時，會收到錯誤**%ASA-4-400024： IDS：2151 Large ICMP packet from to on interface outside**。

解決方案

停用簽名2150和2151以解決此問題。停用簽名後，ping工作正常。

使用以下命令可停用簽名：

ASA(config)#ip audit signature 2151 disable

ASA(config)#ip audit signature 2150 disable

錯誤：- %ASA-4-402119： IPSEC：從remote_IP （使用者名稱）到local_IP收到反重播檢查失敗的協定資料包（SPI=spi，序列號= seq_num）。

問題

我在ASA的日誌消息中收到此錯誤：

錯誤：- %|ASA-4-402119： IPSEC：從remote_IP （使用者名稱）到local_IP收到反重播檢查失敗的協定資料包（SPI=spi，序列號= seq_num）。

解決方案

要解決此錯誤，請使用crypto ipsec security-association replay window-sizecommand改變窗口大小。

<#root>

hostname(config)#

crypto ipsec security-association replay window-size 1024

Cisco建議您使用完整的1024窗口大小來消除任何反重放問題。

錯誤消息- %ASA-4-407001：拒絕本地主機介面名稱：內部地址的

流量，超過許可證數量限制

問題

少量主機無法連線到Internet，並且系統日誌中會顯示以下錯誤消息：

錯誤消息- %ASA-4-407001：拒絕本地主機介面名稱：內部地址的流量，超過許可證數量限制

解決方案

當使用者數目超過使用的授權使用者限制時，會收到此錯誤訊息。此錯誤可透過將許可證升級到更多使用者數來解決。

使用者許可證可以根據需要包括50、100或不限數量的使用者。

錯誤消息- %VPN_HW-4-PACKET_ERROR：

問題

TheError Message - %VPN_HW-4-PACKET_ERROR：錯誤消息表明路由器收到的具有HMAC的ESP資料包不匹配。此錯誤可能由以下問題引起：

- 有缺陷的VPN硬體模組
- ESP資料包損壞

解決方案

若要解決此錯誤訊息：

- 除非發生流量中斷，否則忽略錯誤消息。
- 如果出現流量中斷，請更換模組。

錯誤消息：Command rejected： delete crypto connection between VLAN XXXX and XXXX， first。

問題

當您嘗試在交換機的中繼埠上增加允許的VLAN時，會顯示此錯誤消息：Command rejected： delete crypto connection between VLAN XXXX， first.。

不能修改WAN邊緣中繼以允許其他VLAN。也就是說，您無法在IPSEC VPN SPAtrunk中增加VLAN。

此命令被拒絕，因為它導致一個加密連線的介面VLAN屬於允許的VLAN清單，這可能會造成

IPSec安全漏洞。

請注意，此行為適用於所有中繼埠。

解決方案

不應該使用o switchport trunk allowed vlan (vlanlist)命令，請使用switchport trunk allowed vlan nonecommand或「switchport trunk allowed vlan remove (vlanlist)」命令。

錯誤消息- % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE：丟棄的資料包-會話x.x.x.x：27331到x.x.x.x：23的窗口縮放選項無效[Initiator(flag 0，factor 0) Responder (flag 1， factor 2)]

問題

當您嘗試從VPN隧道遠端的裝置telnet或嘗試從路由器本身telnet時，會發生以下錯誤：

錯誤消息- % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE：丟棄的資料包-會話x.x.x.x：27331到x.x.x.x：23的窗口縮放選項無效[Initiator(flag 0，factor 0) Responder (flag 1， factor 2)]

解決方案

使用者許可證可以根據需要包括50、100或不限數量的使用者。增加了窗口縮放功能，使資料能夠在長距離網路(LFN)上快速傳輸。

這些連線通常具有很高的頻寬，但延遲也很高。

具有衛星連線的網路是LFN的其中一個範例，因為衛星連結通常會有較高的傳輸延遲，但通常會有較高的頻寬。

要啟用窗口縮放功能以支援LFN，TCP窗口大小必須大於65,535。如果將TCP窗口大小增加到大於65,535，則可以解決此錯誤消息。

%ASA-5-305013：為轉發和反向匹配的非對稱NAT規則。請更新此問題流程

問題

一旦VPN隧道啟動，此錯誤消息就會出現：

%ASA-5-305013：為轉發和反向匹配的非對稱NAT規則。請更新此問題流程

解決方案

要解決此問題，當與使用NAT的主機不在同一介面上時，請使用對映地址（而不是實際地址）連線到主機。

此外，如果應用程式嵌入IP地址，請啟用theinspectcommand。

%ASA-5-713068：已收到非常式通知消息： notify_type

問題

如果VPN隧道無法啟動，系統會顯示此錯誤消息：

%ASA-5-713068：已收到非常式通知消息： notify_type

解決方案

出現此消息是由於配置錯誤（即策略或ACL在對等體上未配置為相同時）。

一旦策略和ACL匹配，隧道便不會出現任何問題。

%ASA-5-720012： (VPN-Secondary)無法更新備用裝置上的IPSec故障轉移運行時資料（或） %ASA-6-720012： (VPN-unit)無法更新備用裝置上的IPsec故障轉移運行時資料

問題

當您嘗試升級思科自適應安全裝置(ASA)時，會顯示以下錯誤消息之一：

%ASA-5-720012： (VPN-Secondary)無法更新備用裝置上的IPSec故障轉移運行時資料。

%ASA-6-720012： (VPN-unit)無法更新備用裝置上的IPSec故障轉移運行時資料。

解決方案

這些錯誤訊息是資訊性錯誤。這些消息不會影響ASA或VPN的功能。

當VPN故障切換子系統無法更新與IPsec相關的運行時資料時，這些消息會出現，因為備用裝置上的相關IPsec隧道已被刪除。

為了解決這些問題，請在活動單元上發出wr standbycommand。

錯誤：- %ASA-3-713063：沒有為目標0.0.0.0配置IKE對等體地址

問題

此時顯示**%ASA-3-713063： IKE Peer address not configured for destination 0.0.0.0**錯誤消息，並且隧道無法啟動。

解決方案

如果未為L2L隧道配置IKE對等體地址，則顯示此消息。

如果更改加密對映的序列號，然後刪除並重新應用加密對映，則可以解決此錯誤。

錯誤： %ASA-3-752006：隧道管理器無法排程KEY_ACQUIRE消息。

問題

%ASA-3-752006：隧道管理器無法排程KEY_ACQUIRE消息。加密對映或隧道組的配置可能錯誤。」錯誤消息在Cisco ASA上記錄。

解決方案

此錯誤消息可能是由加密對映或隧道組的配置錯誤引起的。確保兩者都配置正確。有關此錯誤消息的詳細資訊，請參閱錯誤752006。

以下是一些糾正措施：

- 刪除加密ACL（例如，與動態對映關聯）。
- 刪除未使用的IKEv2相關配置（如果有）。
- 驗證加密ACL是否正確匹配。
- 刪除重複的訪問清單條目（如果有）。

錯誤： %ASA-4-402116： IPSEC：從XX.XX.XX.XX (user= XX.XX.XX.XX)到YY.YY.YY.YY接收到ESP資料包(SPI= 0x99554D4E，序列號= 0x9E)

在LAN到LAN VPN隧道設定中，在一端ASA上收到此錯誤：

解除封裝的內部封包與SA中的交涉原則不相符。

資料包將目的地址指定為10.32.77.67，源地址指定為10.105.30.1，協定指定為icmp。

SA將其本地代理指定為10.32.77.67/255.255.255.255/ip/0，並將remote_proxy指定為10.105.42.192/255.255.255.224/ip/0。

解決方案

您需要驗證VPN隧道兩端定義的相關流量訪問清單。兩者必須完全匹配為映象映像。

由於錯誤0xffffffff而未能啟動64位VA安裝程式以啟用虛擬介面卡

問題

當AnyConnect無法連線時，會收到`Failed to launch 64-bit VA installer to enable the virtual adapter due to error 0` xffffffflog message。

解決方案

請完成以下步驟以解決此問題：

1. 轉至System > Internet Communication Management > Internet Communication 設定，並確保Turn Off Automatic Root Certificates 更新已停用。
2. 如果已停用，則請停用已分配到受影響電腦的GPO的整個管理模板部分，然後再次測試。

有關詳細資訊，請參閱關閉自動根證書更新。

在Windows 7中，Cisco VPN客戶端無法與資料卡一起使用

問題

在Windows 7中，Cisco VPN Client無法與資料卡一起使用。

解決方案

安裝在Windows 7上的Cisco VPN Client無法與3G連線一起使用，因為Windows 7電腦上安裝的VPN Client不支援資料卡。

警告：「VPN功能可能根本不起作用」

問題

在嘗試在ASA的外部介面上啟用isakmp期間，會收到此警報消息：

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory.  Performance may start to degrade.
VPN functionality may not work at all.
```

此時，透過ssh訪問ASA。HTTPS已停止，其他SSL客戶端也會受到影響。

解決方案

此問題是由不同模組（如記錄器和加密）的記憶體要求引起的。

確保您沒有thelogging queue 0命令。它使隊列大小設定為8192，並且記憶體分配增加。

在ASA5505和ASA5510等平台中，這種記憶體分配往往會消耗其他模組。

IPSec填充錯誤

問題

收到此錯誤訊息：

```
%ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
     0xXXXXXXX, sequence number= 0xXXXX) from x.x.x.x (user= user) to y.y.y.y with
     incorrect IPsec padding
```

解決方案

出現此問題的原因在於IPSec VPN不使用雜湊演算法進行協商。資料包雜湊可以確保ESP通道的完整性檢查。

因此，在沒有雜湊的情況下，格式錯誤的資料包會被Cisco ASA接受而不被檢測到，並且它會嘗試解密這些資料包。

但是，由於這些資料包的格式不正確，ASA在資料包解密過程中發現缺陷。這會導致出現填充錯誤資訊。

建議在VPN的轉換集中加入雜湊演算法，並確保對等體之間的鏈路具有最小的資料包畸變。

VPN隧道在每18個小時之後斷開

問題

VPN隧道在每18小時之後斷開，即使生命週期設定為24小時。

解決方案

生存時間是SA可用於金鑰重定的最長時間。您在配置中輸入的生存期值與SA的金鑰更新時間不同。

因此，在當前的SA到期之前，必須協商新的SA（對於IPsec則是SA對）。

重新生成金鑰的時間必須始終小於生存時間，以便在第一次重新生成金鑰嘗試失敗時允許進行多次嘗試。

RFC並未指定如何計算重新生成金鑰時間。這由實施者自行決定。

因此，時間因平台而異。某些實現可以使用隨機因子來計算金鑰更新計時器。

例如，如果ASA啟動隧道，則正常情況下它會在64800秒= 86400的75%時重新生成金鑰。

如果路由器啟動，則ASA可以等待更長時間，讓對等體有更多時間啟動金鑰更新。

因此，VPN會話每18小時斷開一次以使用另一個金鑰進行VPN協商是正常的。這不能導致任何VPN丟棄或問題。

重新協商LAN到LAN隧道後無法維持通訊流量

問題

重新協商LAN到LAN隧道後，流量不會得到維護。

解決方案

ASA會監控透過它的每個連線，並根據應用檢查功能在其狀態表中維護一個條目。

透過VPN的加密流量詳細資訊以安全關聯(SA)資料庫的形式進行維護。對於LAN到LAN VPN連線，它維護兩種不同的流量流。

一個是VPN網關之間的加密流量。另一個是VPN網關後面的網路資源與另一端後面的終端使用者之間的流量。

當VPN終止時，此特定SA的流詳細資訊將被刪除。

但是，ASA為此TCP連線維護的狀態表條目由於未執行活動而變得過時，從而阻礙了下載。

這意味著，當使用者應用終止時，ASA仍會保留該特定流的TCP連線。

但是，在TCP空閒計時器過期後，TCP連線會成為閒置連線，並最終超時。

透過引入稱為持續IPSec隧道流量的功能，可解決此問題。

Cisco ASA整合了一條新命令sysopt connection preserve-vpn-flows，以便在VPN隧道重新協商時保留狀態表資訊。

預設情況下，此命令處於停用狀態。要啟用此功能，當L2L VPN從中斷中恢復並重新建立隧道時，Cisco ASA會維護TCP狀態表資訊。

錯誤消息說明已達到加密功能的頻寬

問題

2900系列路由器上收到此錯誤消息：

錯誤： 3月20日10:51:29： %CERM-4-TX_BW_LIMIT：對於帶有securityk9技術包許可證的加密功能，已達到最大Tx頻寬限制85000 Kbps。

解決方案

這是一個已知的問題，因為美國政府發佈了嚴格的準則。

根據此規則，securityk9許可證只能允許速率接近於90 Mbps的負載加密，並且限制到裝置的加密隧道/TLS會話的數量。

有關加密導出限制的詳細資訊，請參閱思科ISR G2 SEC和HSEC許可。

對於Cisco裝置，其派生值為傳入或傳出ISR G2路由器的單向流量小於85Mbps，雙向總流量為170Mbps。

此要求適用於Cisco 1900、2900和3900 ISR G2平台。此命令有助於檢視以下限制：

<#root>

```
Router#
show platform cerm-information

Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED
 ---------------------------------------------------------------
 Resource                      Maximum Limit          Available
 ---------------------------------------------------------------
 Tx Bandwidth(in kbps)         85000                  85000
 Rx Bandwidth(in kbps)         85000                  85000
 Number of tunnels               225                    225
 Number of TLS sessions         1000                   1000
---Output truncated----
```

要避免此問題，請購買HSECK9許可證。「hseck9」功能許可證透過增加的VPN隧道計數和安全語音會話提供增強的負載加密功能。

有關Cisco ISR路由器許可的詳細資訊，請參閱軟體啟用。

問題：即使入站解密流量起作用，IPsec隧道的出站加密流量也會失敗。

解決方案

在IPSec連線上多次重新生成金鑰後發現此問題，但觸發條件尚不清楚。

如果檢查show asp dropcommand的輸出並驗證發出的每個出站資料包的到期VPN情景計數器是否增大，即可確定是否存在此問題。

其他

AG_INIT_EXCH消息顯示在「show crypto isakmp sa」和「debug」命令輸出中

如果未啟動隧道，**AG_INIT**_EXCH消息會出現在show crypto isakmp sacommand和indexbugoutput的輸出中。

原因可能是因為isakmp策略不匹配，或者如果在途中阻止了埠udp 500。

出現調試消息「Received an IPC message during invalid state」

此消息為資訊性消息，與VPN隧道斷開無關。

相關資訊

- ASA和Cisco IOS®：VPN分段
- Cisco ASA 5500系列安全裝置
- IPSec 協商/IKE 通訊協定
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。