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思科技術支援已解決的服務請求。

其中許多解決方案是在IPsec VPN連線的深入故障排除之前實施的。

本文檔提供了在排除連線故障之前需要嘗試的常見步驟的摘要。

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都適用於VPN 3000。

請參閱IP安全性疑難排解 — 瞭解和使用debug命令，以取得用於排解Cisco IOS®軟體和IPsec問題的常見debug命令的說明。

注意：ASA不會通過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臨時丟失裝置上的所有IPsec VPN連線。

建議謹慎實施這些解決方案，並且要符合您的更改控制策略。

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
- Cisco 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解決方案無法正常工作。

當前的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，但可以將這些解決方案用作專案清單，在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，並且已經解決了許多問題。

- 啟用NAT穿越(#1 RA VPN問題)
- 正確測試連通性
- 啟用ISAKMP
- 啟用/禁用PFS
- 清除舊安全關聯或現有安全關聯（隧道）
- 驗證ISAKMP生存期
- 啟用或禁用ISAKMP Keepalive
- 重新輸入或恢復預共用金鑰
- 預共用金鑰不匹配
- 移除並重新應用密碼編譯對應
- 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是否正確且已繫結到加密對映
- 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IP地址是否正確
- 驗證隧道組和組名稱
- 停用L2L對等點的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降到了第二行。

啟用NAT穿越(#1 RA VPN問題)

NAT穿越(或NAT-T)允許VPN流量通過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，但他們無法訪問安全裝置背後的內部網路。

如果沒有在NAT/PAT裝置中啟用NAT-T，則可能會在ASA中收到**protocol 50 src inside:10.0.1.26 dst outside:10.9.69.4**的常規轉換建立失敗錯誤消息。

同樣，如果您無法通過同一IP地址同時登入，則安全VPN**連線會由客戶端在本地終止。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：在Cisco IOS®軟體版本12.2(13)T及更高版本中，Cisco IOS®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。本示例中的二十(20)是保持連線時間（預設值）。

ASA

```
<#root>

securityappliance(config)#

crypto isakmp nat-traversal 20
```

客戶端也需要修改才能正常工作。

在Cisco VPN Client中，導航至Connection Entries，然後點選Modify。它將開啟一個新視窗，您必須在其中選擇「傳輸」(Transporttab)。

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

通過配置ACL來允許NAT-T、UDP 500和ESP埠的UDP 4500非常重要，因為ASA充當NAT裝置。

有關詳細資訊，請參閱使用NAT配置通過防火牆的IPsec隧道，以瞭解有關ASA中ACL配置的詳細資訊。

正確測試連通性

理想的情況下,VPN連線從執行加密的終端裝置後面的裝置測試，但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一般在此用途中有效，但重要的是要從正確的介面獲取ping命令。

如果Ping來源不正確，則可能顯示VPN連線確實工作失敗。範例如下：

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一定源自任一路由器後面的內部網路。這是因為加密ACL僅設定為加密具有這些來源位址的流量。

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命令的擴展選項從路由器的內部介面發出ping:

<#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。用於測試連線性的ping也可源自帶有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ping攻擊安全裝置的內部介面。

如果必須使用ping將內部介面作為目標，則必須在該介面上啟用management-access，否則裝置不會回覆。

```
<#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，指示可能存在不正確的加密對等體配置和/或不正確的ISAKMP建議配置：

<#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，這表示在主模式(MM)下有關狀態交換的失敗。

階段1開啟時的加密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

如果未指示IPsec VPN隧道正常工作，則可能是尚未啟用ISAKMP。請確保已在您的裝置上啟用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(用您所需的介面替換外部)

<#root>

```
securityappliance(config)#
```

crypto isakmp enable outside

在外部介面上啟用ISAKMP時也會收到此錯誤：

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

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

驗證是否保留了UDP 500和4500埠號用於與對等體協商ISAKMP連線。

當介面上未啟用ISAKMP時，VPN客戶端會顯示一條類似以下消息的錯誤消息：

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

為了解決此錯誤，請在VPN網關的加密介面上啟用ISAKMP。

啟用/禁用PFS

在IPsec協商中，完全向前保密(PFS)可確保每個新的加密金鑰與之前的任何金鑰無關。

在隧道對等體上啟用或禁用PFS；否則，ASA/Cisco IOS®路由器中未建立LAN到LAN(L2L)IPsec隧道。

完全轉發保密(PFS)是思科專有技術，第三方裝置不支援。

ASA:

預設情況下，PFS處於禁用狀態。要啟用PFS，請在組策略配置模式下使用帶有enable關鍵字的thepfscommand。要禁用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形式可防止值傳輸。

<#root>

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

no pfs

Cisco IOS®路由器：

要指定在為此加密對映條目請求新的安全關聯時IPsec必須請求PFS，請在加密對映配置模式下使用setpfscommand。

若要指定IPsec在收到新的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。

若要指定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。如果使用此命令未指定組，則group1用作預設值。

```
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

清除舊安全關聯或當前安全關聯（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）。

建立新的SA後，通訊將恢復，因此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（第I階段）和IPsec（第II階段）安全關聯(SA)，則它是解決IPsec VPN問題的最簡單且通常也是最佳解決方案。

如果清除SA，則無需故障排除即可頻繁地解決各種錯誤消息和奇怪行為。

雖然在任何情況下都可以輕鬆使用此技術，但幾乎總是需要在您更改或新增到當前IPsec VPN配置後清除SA。

此外，儘管可以只清除特定的安全關聯，但當您在裝置上全域性清除SA時，最大的好處將隨之產生。

清除安全關聯後，可能需要通過隧道傳送流量來重新建立它們。

警告：除非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它們

    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，也可以使用與命令一起顯示的選項輸入每個命令。

    a. Cisco IOS®

a. ISAKMP（第I階段）

<#root>

```
router#
clear crypto isakmp
 ?
  <0 - 32766>  connection id of SA
  <cr>
```

b. IPsec（第II階段）

<#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（第I階段）

<#root>

```
securityappliance#
clear crypto isakmp sa
```

b. IPsec（第II階段）

<#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生存期

如果使用者經常通過L2L隧道斷開連線，問題可能是ISAKMP SA中配置的生存期較短。

如果ISAKMP生存期內出現任何差異，您可以收到%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。一般情況下，較短的生存期可提供更安全的ISAKMP協商（最多一點），但是，由於生存期較短，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期小於或等於比較的策略中的生存期時，將進行匹配。

如果生存期不同，則使用較短的生存期（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IKE SA未建立。

指定SA生存期。此示例將生存時間設定為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生存期，則在VPN連線終止時收到以下錯誤消息：

安全VPN連線由客戶端在本地終止。原因426：超出配置的最大生命期。

要解決此錯誤消息，請將elifetimevalue設定為0(0)，以便將IKE安全關聯的生存期設定為無窮大。VPN始終處於連線狀態且不會終止。

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

您也可以在群組原則中停用re-xauth，以解決問題。

啟用或禁用ISAKMP Keepalive

如果配置ISAKMP keepalive，將有助於防止偶發丟棄的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之後丟棄的隧道。

此功能允許通道端點監控遠端對等點的持續存在並向該對等點報告其自身的存在狀態。

如果對等體變得無響應，端點將刪除連線。

若要使ISAKMP keepalive正常運作，兩個VPN終端都必須支援它們。

使用以下命令在Cisco IOS®中設定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:

適用於名為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，必須禁用此功能才能解決問題，例如，如果VPN客戶端位於阻止DPD資料包的防火牆後面。

Cisco ASA，適用於名為10.165.205.222的隧道組

禁用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
```

禁用Cisco VPN客戶端4.x的Keepalive

在遇到問題的客戶端PC上導航到%System Root% > Program Files > Cisco Systems > VPN Client > Profiles，以禁用IKE keepalive，並在適用時編輯連線的PCF檔案。

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

Keepalive是思科專有技術，第三方裝置不支援。

重新輸入或恢復預共用金鑰

在許多情況下，當IPsec VPN隧道無法工作時，可能會因為簡單的排版錯誤而造成故障。例如，在安全裝置上，預共用金鑰一旦輸入就會隱藏。

這種混淆使得人們不可能看到金鑰是否不正確。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其正確性；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客戶端和頭端裝置之間的組名或預共用金鑰不匹配，則可能會面臨此錯誤。

```
 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。請謹慎使用這些命令，並在刪除與加密相關的命令之前參閱組織的更改控制策略。

使用以下命令刪除並重新輸入對等體10.0.0.1或grouppngroupin Cisco IOS®的預共用keysecretkeykey:

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
```

使用以下命令刪除並重新輸入/ASA安全裝置上的對等方10.0.0.1的pre-shared-keysecretkeykey:

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隧道的啟動會斷開連線。之所以會出現此問題，是因為第一階段協商中的預共用金鑰不匹配。

show crypto isakmp 命令中的MM_WAIT_MSG_6消息指示預共用金鑰不匹配，如以下示例所示：

<#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

為了解決此問題，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。有關更多資訊，請參見Re-Enter or Recover Pre-Shared-Keyos。

移除並重新應用密碼編譯對應

清除安全關聯時，它不會解決IPsec VPN問題，請刪除並重新應用相關加密對映，以解決各種問題，包括VPN隧道間歇性中斷和某些VPN站點無法啟動。

警告：如果從介面刪除加密對映，其定義將會關閉與該加密對映關聯的任何IPsec隧道。請謹慎執行這些步驟，並在繼續之前考慮組織的更改控制策略。

使用以下命令刪除和替換Cisco IOS®中的加密對映：

從從介面刪除加密對映開始。使用crypto mapcommand的no形式。

```
<#root>

router(config-if)#

no crypto map mymap
```

繼續使用此表單刪除整個加密對映。

```
<#root>

router(config)#

no crypto map mymap 10
```

更換對等裝置10.0.0.1的介面Ethernet0/0上的加密對映。此示例顯示所需的最低加密對映配置：

```
<#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
```

使用以下命令刪除和替換ASA上的加密對映：

從從介面刪除加密對映開始。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。此示例顯示所需的最低加密對映配置：

```
<#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
```

如果您移除並重新應用密碼編譯對應，則當標頭端的IP位址變更時，這也會解決連線問題。

驗證sysopt命令是否存在（僅限ASA）

命令sysopt connection permit-ipsecandsysopt connection permit-vpnallow packets from an IPsec tunnel and their payload to bypass interface ACLs on the security appliance。

如果未啟用這些命令之一，在安全裝置上終止的IPsec隧道可能會失敗。

在安全裝置軟體7.0版及更低版本中，適用於此情況的相關sysopt命令是sysopt connection permit-ipsec。

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

在6.x中，預設情況下禁用此功能。使用/ASA 7.0(1)及更高版本時，預設情況下啟用此功能。使用以下show命令可確定您的設備上是否已啟用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)
```

使用以下命令為您的裝置啟用correctsysoptcommand:

Cisco ASA

<#root>

securityappliance(config)#

sysopt connection permit-vpn

如果不希望使用sopt connectioncommand，請明確允許所需的相關流量從源到目標。

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

驗證ISAKMP身份

如果IPsec VPN隧道在IKE協商中失敗，則失敗可能是因為其對等體無法識別其對等體的身份。

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ISAKMP標識的設定方式，傳送其IP地址或主機名。

預設情況下，防火牆裝置的ISAKMP標識設定為IP地址。

作為一般規則，請以相同方式設定安全裝置及其對等體的身份，以避免IKE協商失敗。

若要設定要傳送到對等體的階段2 ID，請在全域性配置模式下使用isakmp 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.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項失敗，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項失敗，不匹配！

驗證空閒/會話超時

如果閒置逾時設定為30分鐘（預設值），則表示在30分鐘沒有流量通過通道後捨棄該通道。

無論空閒超時引數如何，VPN客戶端都會在30分鐘後斷開連線，**並且會遇到PEER_DELETE-IKE_DELETE_UNSPECIFIED錯誤**。

設定reidle timeoutandsession timeoutasnonein以設定通道alwaysup，如此一來，即使使用第三方裝置，通道也不會被捨棄。

ASA

在組策略配置模式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間：

<#root>

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

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

<#root>

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

當您配置了tunnel-allconfigured時，不需要配置idle-timeout，因為即使您配置了VPN-idle

timeout，它也不會工作，因為所有流量都通過隧道（因為已配置了tunnel-all）。

因此，相關流量（甚至PC生成的流量）是有趣的，不會讓空閒超時生效。

Cisco IOS®路由器

在全域性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，禁用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護SA。seconds引數的有效值範圍為60到86400。

驗證ACL是否正確且已繫結到加密對映

典型IPsec VPN配置中使用了兩個訪問清單。一個訪問清單用於將目的地為VPN隧道的流量從NAT進程中免除。

其他存取清單定義要加密的流量；其中包括LAN到LAN設定中的加密ACL或遠端存取設定中的分割通道ACL。

當這些ACL配置錯誤或遺漏時，流量可能沿一個方向流過VPN隧道，或者根本未通過隧道傳送。

確保在全域組態模式下，使用crypto map match address指令使用密碼編譯對應繫結加密ACL。

請確保您已配置完成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。

當您懷疑ACL是您的IPsec VPN出現問題的原因時，此清單包含一些簡單的檢查內容。

確保NAT免除和加密ACL指定正確的流量。

如果您有多個VPN通道和多個加密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，這表示使用theroute-mapcommand。

在ASA上，這表示您使用thenat(0)命令。LAN到LAN和遠端訪問配置均需要NAT免除ACL。

此處，Cisco IOS®路由器配置為將在192.168.100.0 /24和192.168.200.0 /24或192.168.1.0 /24之間傳送的流量從NAT中免除。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豁免ACL僅能與IP地址或IP網路一起使用(如上述示例（訪問清單noNAT）），並且必須與加密對映ACL相同。

NAT免除ACL不適用於埠號（例如23、25、...）。

在VOIP環境中，網路之間的語音呼叫是通過VPN進行通訊的，如果沒有正確配置NAT 0 ACL，則語音呼叫將無法工作。

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

如果NAT免除(nat 0)ACL中有錯誤配置，您可能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
```

錯誤示例：

<#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，則嘗試將其刪除，然後發出NAT 0命令使其正常工作。

請確保ACL不是向後的，並且它們是正確的型別。

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。

這表示該ACL必須到達其他。在本示例中，在192.168.100.0 /24和192.168.200.0 /24之間設定了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，用於遠端訪問配置的拆分隧道ACL必須作為允許流量進入VPN客戶端需要訪問的網路的標準訪問清單。

Cisco IOS®路由器可以將擴展ACL用於拆分隧道。在擴充存取清單中，在分隔通道ACL的來源處使用「any」與停用分割通道類似。

在延伸型ACL中僅使用來源網路用於分割通道。

正確示例：

```
<#root>

access-list 140 permit ip

10.1.0.0 0.0.255.255

 10.18.0.0 0.0.255.255
```

錯誤示例：

```
<#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
```

ASA 8.3版中站點到站點VPN隧道的NAT豁免配置：

必須在HOASA和BOASA之間建立站點到站點VPN，二者均採用8.3版。HOASA上的NAT免除配置如下所示：

```
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客戶端或站點到站點VPN無法與遠端裝置建立通道，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指定的生存期何時小於或等於啟動器傳送的策略中的生存期。

如果壽命不同，則安全裝置使用較短的壽命。如果不存在可接受的匹配項，ISAKMP將拒絕協商，並且SA未建立。

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

以下是詳細日誌消息：

```
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
```

此消息通常由於ISAKMP策略不匹配或遺漏的NAT 0語句而出現。

此外，系統會顯示以下訊息：

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

此消息表示階段1完成後，階段2消息位於隊列中。此錯誤消息是由以下原因之一導致的：

- 任何對等點的階段不相符
- ACL會阻止對等體完成第1階段

此消息通常出現在**Removing peer from peer table failed, no match!錯誤消息**之後。

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。頭端裝置必須與Cisco VPN客戶端的一個IKE建議匹配。

對於ASA上使用的ISAKMP策略和IPsec轉換集，Cisco VPN客戶端無法使用包含DES和SHA組合的策略。

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）具有正確的路由資訊，以便通過VPN隧道傳送流量。

如果您的網關裝置後面存在其他路由器，請確保這些路由器知道如何到達隧道以及另一端的網路。

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非常有用，因為RRI安裝的路由可以通過路由協定（如EIGRP或OSPF）重分發。

在LAN到LAN配置中，每個端點必須有一條或多條通往網路的路由，這些路由應用於加密流量。

在本例中，路由器A必須具有通過10.89.129.2到路由器B後面的網路的路由。路由器B必須具有通向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已更換為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，則靜態路由的配置將變得難以維護。

相反，建議您按照所述使用反向路由注入。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，並非總是必須更改路由。

但是，如果VPN網關路由器或安全裝置後面存在其他路由器，這些路由器需要以某種方式學習到VPN客戶端的路徑。

在本示例中，假設VPN客戶端在連線時的地址範圍是10.0.0.0 /24。

如果網關與其它路由器之間沒有使用路由協定，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
```

如果在網關和其他路由器之間使用路由協定（如EIGRP或OSPF），則建議按照所述使用反向路由注入。

RRI會自動將VPN客戶端的路由新增到網關的路由表中。然後，可以將這些路由分發到網路中的其

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地址池與頭端裝置的內部網路重疊，則會發生路由問題。有關詳細資訊，請參閱重疊專用網絡部分。

驗證轉換集是否正確

確保兩端轉換集使用的IPsec加密和雜湊演算法相同。

有關詳細資訊，請參閱《思科安全裝置配置指南》的Command參考。

對於ASA上使用的ISAKMP策略和IPsec轉換集，Cisco VPN客戶端無法使用包含DES和SHA組合的策略。

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，並且驗證加密對映是否應用在IPsec隧道啟動/結束的正確介面中

如果靜態對等體和動態對等體配置在同一個加密對映上，則加密對映條目的順序非常重要。

動態加密對映條目的序列號必須高於所有其他靜態加密對映條目。

如果靜態條目的編號高於動態條目的編號，則與這些對等體的連線將失敗，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。

以下是包含靜態專案與動態專案的正確編號密碼編譯對應範例。請注意，動態條目的序列號最高，並且預留空間以新增其他靜態條目：

<#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，也可能出現此錯誤消息。

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發起程式找不到策略：**

在要在同一介面中終止多個VPN隧道的場景中，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。

這適用於路由器和ASA。

同樣，請參閱ASA：向現有L2L VPN新增新隧道或遠端訪問 — Cisco以瞭解有關L2L和遠端訪問VPN方案的加密對映配置的詳細資訊。

驗證對等IP地址是否正確

建立和管理IPsec的特定於連線的記錄的資料庫。

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Remote peer IP Address(remote tunnel end)。

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

使用ASDM配置VPN時，它會自動生成隧道組名稱以及正確的對等IP地址。

如果對等IP地址配置不正確，日誌可能會包含此消息，通過正確配置對等IP地址可解決此消息。

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

當對等體IP地址未在ASA加密配置上正確配置時，ASA無法建立VPN隧道並僅在MM_WAIT_MSG4階段中掛起。

為了解決此問題，請更正配置中的對等IP地址。

以下是show crypto isakmp命令在VPN隧道在MM_WAIT_MSG4狀態下掛起時的輸出。

<#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
```

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，因此丟棄隧道時會顯示此消息。

<#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
```

對預設組策略中已有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對等點的XAUTH

如果在同一個加密對映上設定了LAN到LAN通道和遠端存取VPN通道，則會提示LAN到LAN對等點輸入XAUTH資訊，而LAN到LAN通道在show crypto isakmp saccommand的輸出中會以「CONF_XAUTH」失敗。

以下是SA輸出的範例：

<#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不會受到此問題的影響，因為它使用隧道組。

輸入isakmp金鑰時使用o-xauthkeyword，因此裝置不會提示對等路由器取得XAUTH資訊（使用者名稱和密碼）。

此關鍵字對靜態IPsec對等停用XAUTH。在同一加密對映上配置了L2L和RA VPN的裝置上，輸入類似以下的命令：

<#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，由於Xauth問題，Easy VPN客戶端無法連線到頭端。

在ASA中禁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
```

若要了解有關isakmp ikev1-user-authenticationcommand的更多資訊，請參閱本文檔的Miscellaneoussection部分。

VPN池耗盡

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

1. 刪除現有範圍，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. 將不連續子網新增到VPN池時，可以定義兩個單獨的VPN池，然後在「tunnel-group attributes」下按順序指定它們。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
```

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連線出現延遲問題時，請檢驗以下條件以解決此問題：

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

VPN客戶端無法與ASA連線

問題

將X-auth用於Radius伺服器時，Cisco VPN使用者端無法進行驗證。

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

將X-auth用於Radius伺服器時，Cisco VPN使用者端無法進行驗證。

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
```

如果這能正常運作，則問題與Radius伺服器設定相關。

從ASA檢驗Radius伺服器的連線。如果ping工作正常且沒有任何問題，請檢查ASA上與Radius相關的配置以及Radius伺服器上的資料庫配置。

您可以使用debug指令來疑難排解radius相關問題。有關sampledebug radiusoutput的資訊，請參閱thisSample Output。

在ASA上使用debug命令之前，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「安全VPN連線由對等端終止」。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頻繁丟棄連線

安全VPN連線由對等體終止。理由433。

安全VPN連線由對等項原因終止433：（對等項未指定原因）

已嘗試分配網路或廣播IP地址，正在從池中刪除(x.x.x.x)

解決方案1

問題可能是通過ASA、Radius伺服器、DHCP伺服器或通過充當DHCP伺服器的Radius伺服器分配的IP池。

使用debug加密命令驗證網路掩碼和IP地址是否正確。此外，請確認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適當的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。您必須檢查AAA伺服器以排除此錯誤。

檢查伺服器和客戶端上的伺服器身份驗證密碼。重新載入AAA伺服器可以解決此問題。

解決方案3

此問題的另一種解決方法是禁用威脅檢測功能。

當針對不同的不完整安全關聯(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埠被標籤為主要威脅。

嘗試禁用威脅檢測功能，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
```

這可以用作一種解決方法，以驗證這是否解決了實際問題。

確保在Cisco ASA上禁用威脅檢測實際上會損害幾項安全功能，例如緩解掃描嘗試、使用無效SPI的DoS、Application Inspection失敗的資料包以及Incomplete Sessions。

解決方案4

當轉換集配置不正確時，也會發生此問題。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

遠端訪問使用者一旦連線到VPN就沒有Internet連線。

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

嘗試以下解決方案以解決此問題：

- 無法訪問隔離區中的伺服器
- VPN使用者端無法解析DNS
- Split-Tunnel — 無法訪問Internet或排除的網路
- 本地LAN訪問
- 重疊的專用網路

無法訪問隔離區中的伺服器

一旦使用VPN前端裝置(ASA/Cisco IOS®路由器)建立IPsec隧道，VPN客戶端使用者就可以訪問INSIDE網路(10.10.10.0/24)資源，但他們無法訪問DMZ網路(10.1.1.0/24)。

圖表

檢查頭端裝置中是否新增了Split Tunnel， NO NAT配置，以訪問DMZ網路中的資源。

範例：

ASA配置：

此組態顯示如何設定DMZ網路的NAT豁免，以允許VPN使用者存取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配置新增新條目後，清除NAT轉換。

```
Clear xlate
Clear local
```

驗證:

如果通道已建立，請前往Cisco VPN 使用者端，然後選擇Status > Route 詳細資訊，檢查是否顯示DMZ和INSIDE網路的安全路由。

請參閱ASA：向現有L2L VPN新增新隧道或遠端訪問 — Cisco，瞭解將新VPN隧道或遠端訪問VPN新增到已存在的L2L VPN配置所需的步驟。

請參閱ASA：允許在ASA配置上為VPN客戶端分割隧道示例，瞭解有關如何允許VPN客戶端在通過隧道連線到Cisco 5500系列自適應安全裝置(ASA)時訪問網際網路的逐步說明。

VPN使用者端無法解析DNS

建立通道後，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。必須在組策略下配置DNS伺服器配置，並在隧道組常規屬性的組策略下應用；例如：

<#root>

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1) !---
```

```
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客戶端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上啟用拆分DNS配置以解決此問題。

Split-Tunnel — 無法訪問Internet或排除的網路

分割隧道允許遠端訪問IPsec客戶端有條件地以加密形式通過IPsec隧道將資料包定向到網路介面，或者以明文形式將其解密，然後將其路由到最終目的地。

分割通道預設會停用，會偵測流量。

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

只有思科VPN客戶端（而不是EZVPN客戶端）才支援excludespecified選項。

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

如需分割通道的詳細設定範例，請參閱以下檔案：

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

髮夾溶液

對於進入介面但隨後從同一介面路由出去的VPN流量，此功能非常有用。

例如，在集中星型VPN網路中，安全裝置是中心，遠端VPN網路是分支，分支到分支的通訊流量必須進入安全設備，然後再次流向其他分支。

使用same-security-traffic配置允許流量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且只能連線到本地網路。

有關更詳細的配置示例，請參閱ASA：允許VPN客戶端的本地LAN訪問。

重疊的專用網路

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的內部網路重疊的VPN客戶端的IP地址。

解決方案

驗證要為VPN客戶端、前端裝置的內部網路和VPN客戶端內部網路分配的池中的IP地址是否位於不同的網路中。

您可以將相同的主要網路分配給不同的子網，但有時會出現路由問題。

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

無法連線三個以上的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，將顯示以下錯誤消息：

```
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。

嘗試以下解決方案以解決此問題：

- 配置同時登入
- 使用CLI配置ASA
- 配置配置

配置同時登入

如果選中了ASDM中的Inheritcheck框，則使用者僅允許預設同時登入數。同時登入的預設值為三(3)。

為了解決此問題，請增加同時登入的值。

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

   此欄位的最小值為零(0)，這將禁用登入並阻止使用者訪問。

   當您使用來自不同PC的相同使用者帳戶登入時，當前會話（從使用相同使用者帳戶的另一台PC建立的連線）將終止，並且新會話將建立。

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。在該示例中，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更多資訊，請參閱思科安全裝置命令參考。

在全域性配置模式下使用vpn-sessiondb max-session-limitcommand，將VPN會話限製為低於安全裝置允許的值。

使用此命令的輸出可移除作業階段限制。再次使用命令以覆蓋當前設定。

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

此示例說明如何將最大VPN會話限制設定為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

完成這些步驟，以便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，然後將登入次數更改為5。

建立通道後，無法啟動會話或應用並傳輸緩慢

問題

建立IPsec通道後，應用或作業階段不會透過通道啟動。

解決方案

使用ping命令檢查網路或查詢是否可從網路訪問應用伺服器。

對於穿越路由器或/ASA裝置的臨時資料包（尤其是已設定SYN位元的TCP資料段），它可能是一個最大資料段大小(MSS)問題。

Cisco IOS®路由器 — 更改路由器外部介面（隧道端介面）中的MSS值

運行以下命令，以變更路由器外部介面（通道端介面）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)]
```

路由器上的MSS將調整為已配置的1300。

有關詳細資訊，請參閱ASA和Cisco IOS®:VPN分段。

ASA — 請參閱/ASA文檔

無法正確存取Internet或通道傳輸速度緩慢，因為它會顯示MTU大小錯誤訊息和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

您不能從ASA介面啟動VPN隧道，並且在建立隧道後，遠端終端/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隧道啟動到介面內部的ASA的SSH或HTTP連線。

解決方案

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

```
<#root>

ASA-02(config)#

management-access inside


ASA-02(config)#

show management-access

management-access inside
```

此命令還有助於通過VPN隧道向ASA內部介面進行ssh啟動或http連線。

此資訊對DMZ介面同樣適用。例如，如果您想對/ASA的DMZ介面執行ping操作，或者想從DMZ介面啟動隧道，則需要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埠已開啟。

但是，如果這些埠未開啟，請嘗試在TCP埠上連10000，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，也會發生此問題。為了解決此問題，請重新配置VPN隧道。

當資料未加密，但僅通過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
```

為了解決此問題，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通過內部的外介面。輸出示例顯示，解密已完成，但加密未發生。
3. 如果在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將加密/VPN流量從介面ACL檢查中排除。

在同一加密對映上為vpn隧道配置備份對等體

問題

您想對單個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回退清單。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。

如果該對等體不響應，則安全裝置會沿著清單向下移動，直到對等體響應或者清單中不再有對等體。

ASA具有已配置為主對等體的加密對映。可以在主要對等體之後新增輔助對等體。

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

禁用/重新啟動VPN隧道

問題

要暫時禁用VPN隧道並重新啟動服務，請完成本節中介紹的步驟。

解決方案

在全域性配置模式下使用crypto map interface命令將之前定義的加密對映集刪除到介面。

使用此命令的enoform可從介面移除密碼編譯對應集。

<#root>

hostname(config)#

no crypto map

map-name

interface

interface-name

此命令刪除到任何活動安全裝置介面的加密對映集，並使該介面中的IPsec VPN隧道處於非活動狀態。

要在介面上重新啟動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

某些通道未加密

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

之所以會出現此問題，是因為ASA無法通過隧道傳遞加密資料包。在ASP表中建立重複的加密規則。

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

出現**%ASA-5-713904: Group = DefaultRAGroup，IP = 192.0.2.0,...不受支援的事務模式v2 version.Tunnel terminatederror**消息。

解決方案

事務模式v2錯誤消息的原因是ASA僅支援IKE模式配置V6，而不支援舊的V2模式版本。

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傳輸大型資料包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

此日誌消息表明已將大型資料包傳送到客戶端。封包的來源不知道使用者端的MTU。

這也可能是由於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，這樣可以解決此問題。

在VPN隧道的一端啟用QoS時的錯誤消息

問題

如果在VPN隧道的一端啟用了QoS，則可能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

此訊息通常在通道的一端執行QoS時產生。當檢測到資料包順序有誤時，會發生這種情況。

您可以停用QoS來停止此行為，但只要流量能夠穿過通道，就可以忽略此行為。

警告：加密對映條目不完整

問題

執行crypto map mymap 20 ipsec-isakmpcommand時，可能會收到以下錯誤：

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

這是定義新的加密對映時的常見警報；提醒必須在配置引數(如訪問清單（匹配地址）、轉換集和對等體地址)後才能正常工作。

您為定義密碼編譯對應而鍵入的第一行未顯示在配置中也是正常的。

錯誤：- %ASA-4-400024: IDS:2151大ICMP資料包從到外部介面

問題

無法通過vpn隧道傳遞大ping資料包。嘗試傳遞大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

禁用簽名2150和2151以解決此問題。禁用簽名後，ping工作正常。

使用以下命令以停用簽名：

ASA(config)#ip審核簽名2151禁用

ASA(config)#ip審核簽名2150禁用

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

問題

我在ASA的日誌消息中收到此錯誤：

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

解決方案

要解決此錯誤，請使用crypto ipsec security-association replay window-sizecommand更改視窗大小。

<#root>

hostname(config)#

crypto ipsec security-association replay window-size 1024

思科建議您使用完整的1024視窗大小來消除任何反重播問題。

錯誤消息 — %ASA-4-407001：拒絕本地主機介面名稱：inside_address的流量，超出許可證數量限制

問題

少數主機無法連線到Internet，系統日誌中將顯示以下錯誤消息：

錯誤消息 — %ASA-4-407001：拒絕本地主機介面名稱：inside_address的流量，超出許可證數量限制

解決方案

當使用者數超過使用的許可證的使用者限制時，會收到此錯誤消息。可通過將許可證升級到更多使用者來解決此錯誤。

使用者許可證可根據需要包括50、100或不限使用者。

錯誤消息 — %VPN_HW-4-PACKET_ERROR:

問題

錯誤消息 — %VPN_HW-4-PACKET_ERROR：錯誤消息表示路由器接收的ESP資料包與HMAC不匹配。此錯誤可能是由以下問題導致的：

- 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：命令拒絕：首先刪除VLAN XXXX和XXXX之間的加密連線。

問題

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

無法修改WAN邊緣中繼以允許其他VLAN。也就是說，您無法在IPSEC VPN SPAtrunk中新增VLAN。

此命令被拒絕，因為它會導致屬於允許VLAN清單的加密連線介面VLAN，從而可能導致IPSec安全漏洞。

請注意，此行為適用於所有中繼埠。

解決方案

請改用switchport trunk allowed vlan(vlanlist)命令而不是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:27331到x.x.x.x:23的無效視窗縮放選項[Initiator(flag 0,factor 0)Responder(flag 1, factor 2)]

問題

當您嘗試從VPN通道遠端的裝置telnet時，或當您嘗試從路由器本身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:27331到x.x.x.x:23的無效視窗縮放選項[Initiator(flag 0,factor 0)Responder(flag 1, factor 2)]

解決方案

使用者許可證可根據需要包括50、100或不限使用者。新增了視窗縮放功能，可以在長距離網路(LFN)上快速傳輸資料。

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的一個例子，因為衛星連結的傳播延遲總是很高，但通常具有高頻寬。

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

%ASA-5-305013：為正向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，就會出現以下錯誤消息：

%ASA-5-305013：為正向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，如果應用程式嵌入了IP地址，請啟用inspectcommand。

%ASA-5-713068：已收到非例行程式通知消息： notify_type

問題

如果VPN隧道無法啟動，則會出現以下錯誤消息：

%ASA-5-713068：已收到非例行程式通知消息： notify_type

解決方案

出現此消息是因為配置錯誤（即策略或ACL未在對等體上配置為相同時）。

一旦策略和ACL匹配，隧道就會正常運作。

%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，將出現以下錯誤消息之一：

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

%ASA-6-720012：（VPN單元）無法更新備用單元上的IPsec故障轉移運行時資料。

解決方案

這些錯誤消息是資訊性錯誤。這些消息不會影響ASA或VPN的功能。

當VPN故障轉移子系統由於已在備用裝置上刪除相關IPsec隧道而無法更新與IPsec相關的運行時資料時，將顯示這些消息。

為了解決這些問題，請在作用中裝置上發出wr standbycommand。

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

問題

出現「**%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

當未為L2L隧道配置IKE對等地址時，將出現此消息。

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。加密對映或隧道組可能配置錯誤。"在Cisco ASA上記錄錯誤消息。

解決方案

此錯誤消息可能是由於加密對映或通道組的配置錯誤造成的。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(使用者= XX.XX.XX.XX)接收到YY.YY.YY.YY的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：

解除封裝的內部資料包與SA中的協商策略不匹配。

封包將其目的地指定為10.32.77.67，其來源指定為10.105.30.1，其通訊協定指定為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，無法啟動64位VA安裝程式以啟用虛擬介面卡

問題

由於AnyConnect連線失敗時收到錯誤0xffffffflog消息，無法啟動64位VA安裝程式以啟用虛擬介面卡。

解決方案

完成以下步驟即可解決此問題：

1. 轉至System > Internet Communication Management > Internet Communication settings，確保Turn Off Automatic Root Certificates Updateis被禁用。
2. 如果禁用該選項，則禁用分配給受影響電腦的GPO的整個管理模板，然後重新測試。

如需詳細資訊，請參閱關閉自動根憑證更新。

Windows 7上的Cisco VPN客戶端無法與資料卡配合使用

問題

Cisco VPN Client在Windows 7上不能與資料卡配合使用。

解決方案

Windows 7上安裝的Cisco VPN客戶端無法與3G連線配合使用，因為Windows 7電腦上安裝的VPN客戶端不支援資料卡。

警報：「VPN功能可能根本無法工作」

問題

在嘗試在ASA的外部介面上啟用isakmp期間，會收到以下警報消息：

```
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，通過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。

請確保沒有logging queue 0命令。它將隊列大小設定為8192，並且記憶體分配會增加。

在ASA5505和ASA5510等平台中，這種記憶體分配傾向於導致記憶體不足的其他模組。

IPSec填充錯誤

問題

收到以下錯誤消息：

```
%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

發生此問題的原因是IPSec VPN協商時沒有雜湊演算法。資料包雜湊可以確保ESP通道的完整性檢查。

因此，如果不使用雜湊，Cisco ASA將接受格式不正確的資料包，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，因此ASA在資料包解密過程中發現缺陷。這會導致出現填充錯誤消息。

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隧道每18小時斷開一次

問題

VPN隧道每18小時斷開一次，即使其生存時間設定為24小時。

解決方案

生存期是SA可用於重新生成金鑰的最長時間。您在配置中輸入的lifetime值與SA的重新生成金鑰時間不同。

因此，在當前的SA過期之前，必須協商新的SA（對於IPsec來說是SA對）。

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

RFC沒有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。一些實現可以使用隨機因子來計算重新生成計時器。

例如，如果ASA啟動隧道，則通常在64800秒= 75%的時間重新86400鑰。

如果路由器啟動，則ASA可以等待更長時間以給對等方更多時間啟動重新生成金鑰。

因此，VPN會話通常每18小時斷開一次，以使用另一個金鑰進行VPN協商。這不能導致任何VPN丟棄或問題。

重新協商LAN到LAN通道後，流量不會得到維護

問題

重新協商LAN到LAN通道後，流量不會得到維護。

解決方案

ASA監控通過它的每個連線，並根據應用檢查功能在其狀態表中維護一個條目。

通過VPN的加密流量詳細資訊以安全關聯(SA)資料庫的形式維護。對於LAN到LAN VPN連線，它維護兩個不同的流量流。

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

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連線維護的狀態表項因沒有活動而變得過時，從而阻礙了下載。

這意味著，在使用者應用程式終止時，ASA仍保留該特定流的TCP連線。

但是，在TCP空閒計時器過期後，TCP連線將丟失，並最終超時。

通過引入名為Persistent IPSec Tunneled Flows的功能，已解決了此問題。

新的命令sysopt connection preserve-vpn-flows已整合到Cisco ASA中，以便在VPN隧道的重新協商時保留狀態表資訊。

預設情況下，此命令處於禁用狀態。為此，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。

錯誤訊息指出已達到密碼編譯功能的頻寬

問題

2900系列路由器上收到以下錯誤訊息：

錯誤： 3月20日10:51:29: %CERM-4-TX_BW_LIMIT：對於具有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

這是一個眾所周知的問題，因為美國政府發佈了嚴格的准則。

根據要求，securityk9許可證僅允許速率接近90 Mbps的負載加密，並限制到裝置的加密隧道/TLS會話數量。

有關加密匯出限制的詳細資訊，請參閱Cisco ISR G2 SEC和HSEC許可。

對於Cisco裝置，ISR G2路由器傳入或傳出的單向流量小於85 Mbps，雙向總流量為170 Mbps。

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」功能許可證提供增強的負載加密功能，增加了VPN隧道計數和安全語音會話。

有關Cisco ISR路由器許可的詳細資訊，請參閱軟體啟用。

問題：IPsec隧道中的出站加密流量失敗，即使入站解密流量工作正常。

解決方案

在IPsec連線上多次重新生成金鑰後發現此問題，但觸發條件不清楚。

如果您檢查show asp 丟棄命令的輸出，並驗證傳送的每個出站資料包的Expired VPN上下文計數器是否增加，則可能會確定存在此問題。

其他

AG_INIT_EXCH消息出現在「show crypto isakmp sa」和「debug」命令輸出中

如果通道未啟動，則**AG_INIT_EXCH**消息也會出現在show crypto isakmp saccommand和indebugoutput的輸出中。

原因可能是因為isakmp策略不匹配，或者是因為途中阻止了埠udp 500。

出現「Received an IPC message during invalid state（在無效狀態期間收到IPC消息）」調試消息

此消息是資訊性消息，與VPN隧道的斷開無關。

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）。