思科網路層加密配置和故障排除：背景 — 第1部分

目錄

簡介

本文討論使用IPSec和網際網路安全關聯和金鑰管理通訊協定(ISAKMP)來設定和疑難排解Cisco網路層加密，並涵蓋網路層加密背景資訊和基本設定以及IPSec和ISAKMP。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據軟體和硬體版本：

- Cisco IOS®軟體版本11.2及更新版本

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

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

網路層加密背景資訊和配置

網路層加密功能是在Cisco IOS®軟體版本11.2中匯入。它為安全資料傳輸提供了一種機制，包含兩個元件：

- **路由器身份驗證：**在通過加密流量之前，兩台路由器使用數位簽章標準(DSS)公鑰執行一次雙向身份驗證，以便對隨機挑戰進行簽名。
- **網路層加密：**對於IP負載加密，路由器使用Diffie-Hellman金鑰交換來安全地生成DES（40位或56位會話金鑰）、三重DES - 3DES（168位），或最新高級加密標準 — AES（128位（預設），或192位或256位金鑰）(12.2(13)T中引入)。以可配置的方式生成新的會話金鑰。加密策略由加密對映設定，加密對映使用擴展IP訪問清單來定義要在路由器之間加密的網路、子網、主機或協定對。

加密背景

密碼學領域涉及保持通訊的私密性。在密碼學發展的歷史上，保護敏感通訊一直是密碼學研究的重點。加密是將資料轉換為某種不可讀形式。它的目的是通過隱藏資訊，不讓任何人知道它並不想洩露給誰（即使他們能看到加密的資料），來確保隱私。解密與加密相反：它是將加密資料轉換回可理解的形式。

加密和解密需要使用一些秘密資訊，通常稱為「金鑰」。 根據所用的加密機制，同一金鑰可能同時用於加密和解密；但對於其他機制，用於加密和解密的金鑰可能不同。

數位簽章將文檔繫結到特定金鑰的擁有者，而數字時間戳將文檔繫結到在特定時間的建立。這些加密機制可用於控制對共用磁碟驅動器、高安全性安裝或按次付費電視頻道的訪問。

隨著現代密碼學日益多樣化，密碼學從根本上講是建立在難以解決的問題上的。問題可能很難，因為其解決方案要求知道金鑰，例如解密加密的消息或簽署某個數字文檔。該問題也可能很困難，因為它從本質上來說難以完成，例如找到產生給定雜湊值的消息。

隨著密碼學領域的發展，什麼是密碼學、什麼是非密碼學的分界線越來越模糊。當今的密碼學可以概括為對依賴於難以解決的數學問題的存在性的技術和應用的研究。密碼分析師試圖破壞加密機制，而密碼學是密碼學與密碼分析相結合的學科。

定義

本節定義本文檔中使用的相關術語。

- **驗證:**知道所接收的資料是由聲稱的傳送者實際傳送的屬性。
- **機密性：**通訊的特性，使目標收件人知道要傳送的內容，但非目標方無法確定要傳送的內容。
- **資料加密標準(DES):**DES使用對稱金鑰方法，也稱為金鑰方法。這意味著如果資料塊使用金鑰加密，則加密塊必須使用相同的金鑰解密，因此加密器和解密器必須使用相同的金鑰。儘管加密方法已為人所知並已被廣泛採用，但最廣為人知的攻擊方法是通過暴力破解。必須根據加密的塊測試金鑰，以檢視它們是否可以正確解析金鑰。隨著處理器功能的增強，DES的自然壽命已接近尾聲。例如，使用來自網際網路上數千台電腦的空閒處理能力的合作努力，能夠在21天內找到DES編碼消息的56位金鑰。DES每五年由美國國家安全域性進行驗證，以滿足美國政府的目的。目前的批准將於1998年到期，NSA已表示不會重新認證DES。除了DES之外，還有其它加密演算法，除了暴力攻擊之外，它們沒有任何已知的弱點。有關其他資訊，請參閱美國國家標準與技術研究所(NIST)的DES FIPS 46-2 。
- **解密：**對加密資料反向應用加密演算法，從而將資料恢復到其原始的未加密狀態。
- **DSS和數位簽章演演算法(DSA):**DSA由NIST在數位簽章標準(DSS)中發佈，這是美國政府Capstone專案的一部分。DSS被NIST與NSA合作選為美國政府的數字認證標準。該標準於1994年5月19日發佈。
- **加密：**對資料應用特定的演算法，以改變資料的外觀，使無權看到資訊的人無法理解資料。
- **完整性：**確保資料從源傳輸到目的裝置的屬性，不會出現未檢測到的更改。
- **不可否認性：**接收者的屬效能夠證明某些資料的傳送者確實傳送了資料，即使傳送者以後可能希望否認曾傳送過該資料。
- **公鑰加密：**傳統的密碼學是基於消息的傳送者和接收者知道並使用相同的金鑰。傳送方使用金鑰加密消息，接收方使用相同的金鑰解密消息。這種方法稱為「金鑰」或「對稱加密」。 主要問題是讓傳送者和接收者就金鑰達成一致，而其他人不會發現。如果他們位於不同的物理位置，則必須信任快遞員、電話系統或其他傳輸介質，以防止洩漏通訊中的金鑰。任何在傳送過程中偷聽或擷取金鑰的人以後都可以讀取、修改和偽造所有使用該金鑰加密或進行身份驗證的消息。金鑰的產生、傳輸和儲存稱為金鑰管理；所有加密系統都必須處理金鑰管理問題。由於金鑰加密系統中的所有金鑰都必須保持秘密，所以金鑰加密通常很難提供安全的金鑰管理，特別是在具有大量使用者的開放系統中。1976年Whitfield Diffie和Martin Hellman提出公鑰密碼的概念，以解決金鑰管理問題。在他們的概念中，每個人獲得一對金鑰，一個稱為公鑰，另一個稱為私鑰。每個人的公鑰都會被公佈，而私鑰則被保密。傳送方和接收方無需共用秘密資訊，所有通訊都只涉及公鑰，並且不會傳輸或共用私鑰。不再有必要相信某些通訊管道是安全的，以防止竊聽或背叛。唯一的要求是公鑰以受信任（身份驗證）的方式與其使用者相關聯（例如，在受信任的目錄中）。 任何人都可以通過使用公共資訊來傳送機密消息，但是該消息只能使用專用金鑰解密，而專用金鑰由預定收件人獨有。此外，公開金鑰加密不僅可用於隱私（加密），還可用於身份驗證（數位簽章）。
- **公開金鑰數位簽章：** 為了對消息進行簽名，使用者會執行同時涉及其私鑰和消息本身的計算。輸出稱為數位簽章，並附加到消息，然後傳送該消息。第二人通過執行涉及消息、所聲稱的簽名和第一人的公鑰的計算來驗證簽名。如果結果恰當地符合一個簡單的數學關係，則驗證簽名是真實的。否則，簽名可能是欺詐的，或者消息可能已被更改。
- **公開金鑰加密：**當一個人希望向另一個人傳送秘密消息時，第一個人會在目錄中查詢第二個人的公鑰，使用該公鑰加密消息並將其傳送。然後第二個人使用他們的私鑰解密並讀取消息。沒有人可以解密消息。任何人都可以向第二人傳送加密消息，但只有第二人可以閱讀該消息。顯然，一個要求是沒有人可以從相應的公鑰中找出私鑰。
- **流量分析：**分析網路流量，以得出對攻擊者有用的資訊。此類資訊的示例包括傳輸頻率、轉換方的身份、資料包大小、使用的流識別符號等。

初步資訊

本節將討論一些基本的網路層加密概念。它包含您應該關注的加密方面。最初，這些問題可能對您

來說沒有意義，但是現在仔細閱讀並留意它們是一個好主意，因為在使用加密技術幾個月之後，這些問題將更為合理。

- 必須注意的是，加密僅發生在介面的輸出上，而解密僅發生在輸入介面時。在規劃政策時，這種區別很重要。加密和解密策略是對稱的。這意味著定義一個會自動給出另一個。使用加密對映及其關聯的擴展訪問清單，僅顯式定義加密策略。解密策略使用相同的資訊，但是在匹配資料包時，它將反轉源地址和目的地址以及埠。這樣，資料在雙工連線的兩個方向上都受到保護。**crypto map**命令中的*match address x*語句用於描述離開介面的資料包。換句話說，它描述的是資料包的加密。但是，當資料包進入介面時，也必須匹配資料包進行解密。這是通過遍歷訪問清單自動完成的，源地址和目的地址與埠顛倒。這為連線提供了對稱性。**密碼編譯對應**指向的存取清單應只描述一個（傳出）方向的流量。與您定義的訪問清單不匹配的IP資料包將被傳輸，但不會加密。存取清單中的「deny」表示不應匹配這些主機，這表示它們不會加密。在此上下文中，「deny」並不表示封包遭捨棄。
- 請務必小心在延伸存取清單中使用單詞「any」。使用「any」會導致流量被丟棄，除非流量流向匹配的「取消加密」介面。此外，使用Cisco IOS軟體版本11.3(3)T中的IPSec，不允許「any」。
- 在指定源或目標地址時，不建議使用「any」關鍵字。指定「any」可能導致路由協定、網路時間協定(NTP)、回應、回應響應和組播流量出現問題，因為接收路由器會以靜默方式丟棄此流量。如果要使用「any」，對於未加密的流量，應在其前面加上「deny」語句，例如「ntp」。
- 為節省時間，請確保您可以**ping**您嘗試與其建立加密關聯的對等路由器。此外，在花費太多時間排除錯誤問題之前，讓終端裝置（取決於對其流量進行加密）相互執行ping。換句話說，在嘗試進行加密之前，請確保路由**有效**。遠端對等體可能沒有出口介面的路由，在這種情況下，您無法與該對等體進行加密會話(您可能可以在該串列介面上使用**ip unnumbered**)。
- 許多WAN點對點連結使用不可路由的IP位址，而Cisco IOS軟體版本11.2加密依賴網際網路控制訊息通訊協定(ICMP)（表示為ICMP使用輸出序列介面的IP位址）。 這可能會強制在WAN介面上使用**ip unnumbered**。請一律執行**ping**和**traceroute**命令，以確保兩個對等（加密/解密）路由器的路由就位。
- 只允許兩台路由器共用Diffie-Hellman會話金鑰。也就是說，一台路由器無法使用相同的會話金鑰將加密資料包交換給兩個對等體；每對路由器必須有一個會話金鑰，這是它們之間的Diffie-Hellman交換的結果。
- 加密引擎位於Cisco IOS、VIP2 Cisco IOS中或者位於VIP2上的加密服務介面卡(ESA)硬體中。如果沒有VIP2,Cisco IOS加密引擎將管理所有埠的加密策略。在使用VIP2的平台上，有多個加密引擎：cisco IOS中一個，每個VIP2一個。VIP2上的加密引擎控制主機板上埠的加密。
- 確保流量設定為到達準備加密的介面。如果流量可能以某種方式到達應用了加密對映**的介面**以外的介面，則會以靜默方式丟棄該流量。
- 它有助於在進行金鑰交換時讓控制檯（或備用）訪問兩台路由器；可以在等待金鑰時使被動端掛起。
- **cfb-64**比**cfb**-8更有效**地處理**CPU負載。
- 路由器需要運行要用於要使用的密碼反饋(CFB)模式的演算法；每個映像的預設值是使用**cfb-64**的映像名稱（例如「56」）。
- 考慮更改key-timeout。30分鐘的預設時間非常短。嘗試將其增加為一天（1440分鐘）。
- 每次金鑰到期時，金鑰重新協商期間都會丟棄IP流量。
- 僅選擇您真正想要加密的流量（這樣可以節省CPU週期）。
- 透過按需撥號路由(DDR)，讓ICMP變得有趣，否則它永遠不會撥出。
- 如果要加密IP以外的流量，請使用通道。透過通道，將密碼編譯對應套用到實體和通道介面。請參閱範例5:加密IP通道中的IPX流量以瞭解詳細資訊。
- 兩個加密對等路由器不需要直接連線。
- 低端路由器可能會顯示「CPU佔用」消息。可以忽略這一點，因為它告訴您加密佔用大量

CPU資源。
- 請勿將加密路由器設定為冗餘格式，以便解密、重新加密流量並浪費CPU。只需在兩個端點進行加密。請參閱範例3:透過路由器加密以瞭解詳細資訊。
- 目前，不支援對廣播和組播資料包進行加密。如果「安全」路由更新對網路設計很重要，則應使用內建身份驗證的協定，如增強型內部網關路由協定(EIGRP)、開放最短路徑優先(OSPF)或路由資訊協定版本2(RIPv2)來確保更新的完整性。

注意事項

注意：下面提到的警告均已解決。

- 使用ESA進行加密的Cisco 7200路由器無法在一個會話金鑰下解密資料包，然後在另一個會話金鑰下重新加密該資料包。請參閱Cisco錯誤ID CSCdj82613(僅限註冊客戶)。
- 當兩台路由器通過加密租用線路和ISDN備用線路連線時，如果租用線路斷開，ISDN鏈路可以正常運作。但是，當租用線路再次恢復時，發出ISDN呼叫的路由器崩潰。請參閱Cisco錯誤ID CSCdj00310(僅限註冊客戶)。
- 對於具有多個VIP的Cisco 7500系列路由器，如果對任何VIP的一個介面都應用了**加密對映**，則一個或多個VIP將崩潰。請參閱Cisco錯誤ID CSCdi88459(僅限註冊客戶)。
- 對於具有VIP2和ESA的Cisco 7500系列路由器，除非使用者位於控制檯埠，否則**show crypto card**命令不顯示輸出。請參閱Cisco錯誤ID CSCdj89070(僅限註冊客戶)。

Cisco IOS網路層加密組態

本文檔中的工作Cisco IOS配置示例直接來自實驗路由器。唯一的改變是刪除了無關的介面配置。此處的所有資料均來自Internet上的免費資源，或本文檔末尾的相關資訊部分。

本文檔中的所有配置示例均來自Cisco IOS軟體版本11.3。Cisco IOS軟體版本11.2命令進行了多項更改，例如新增了以下文字：

- 某些關鍵配置命令中的DSS。
- cisco使用一些**show**命令和**crypto map**命令來區分Cisco的專有加密（如Cisco IOS軟體版本11.2及更高版本中所示）和Cisco IOS軟體版本11.3(2)T中的IPSec。

注意：這些配置示例中使用的IP地址是在思科實驗室中隨機選擇的，旨在完全通用。

第1步：手動生成DSS金鑰對

需要在參與加密會話的每個路由器上手動生成DSS金鑰對（公共金鑰和私有金鑰）。換句話說，每台路由器都必須具有自己的DSS金鑰才能參與。加密引擎只能有一個DSS金鑰來唯一標識它。在Cisco IOS軟體版本11.3中新增了關鍵字「dss」，以便區分DSS和RSA金鑰。您可以為路由器自己的DSS金鑰指定任何名稱（不過，建議使用路由器主機名）。 在功能較弱的CPU（例如Cisco 2500系列）上，生成金鑰對大約需要5秒或更短。

路由器產生一對金鑰：

- 公鑰（稍後會傳送到參與加密會話的路由器）。
- 私鑰(不與其他人看到或交換；實際上，它儲存在NVRAM的單獨部分中（無法檢視）。

路由器的DSS金鑰對生成後，即會與該路由器中的加密引擎唯一關聯。金鑰對生成顯示在下面的示例命令輸出中。

```
dial-5(config)#crypto key generate dss dial5
Generating DSS keys ....
 [OK]

dial-5#show crypto key mypubkey dss
crypto public-key dial5 05679919
 160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F
 F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145
quit


dial-5#show crypto engine configuration
slot:               0
engine name:        dial5
engine type:        software
serial number:      05679919
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    43
input queue bot:    43
input queue count:  0

dial-5#
```

由於您只能生成一個標識路由器的金鑰對，因此可能會覆蓋原始金鑰，並且需要將您的公鑰重新傳送到加密關聯中的每個路由器。如下面的示例命令輸出所示：

```
StHelen(config)#crypto key generate dss barney
% Generating new DSS keys will require re-exchanging
   public keys with peers who already have the public key
   named barney!
Generate new DSS keys? [yes/no]: yes
Generating DSS keys ....
 [OK]


StHelen(config)#
Mar 16 12:13:12.851: Crypto engine 0: create key pairs.
```

第2步：與對等點手動交換DSS公鑰（帶外）

生成路由器自己的DSS金鑰對是建立加密會話關聯的第一步。下一步是與其它每台路由器交換公鑰。您可以手動輸入這些公鑰，方法是先輸入**show crypto mypubkey**命令以顯示路由器的DSS公鑰。然後交換這些公鑰（例如透過電子郵件），並使用**crypto key pubkey-chain dss**指令，將對等路由器的公鑰剪下並貼上到路由器中。

您還可以使用**crypto key exchange dss** 命令讓路由器自動交換公鑰。如果使用自動方法，請確保用於金鑰交換的介面上沒有**crypto map**語句。**debug crypto key**在此處有用。

注意：在嘗試交換金鑰之**前**對您的對等體執行ping操作是個好主意。

```
Loser#ping 19.19.19.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds:
!!!!!
```

```
Loser(config)#crypto key exchange dss passive
Enter escape character to abort if connection does not complete.
Wait for connection from peer[confirm]
Waiting ....


  StHelen(config)#crypto key exchange dss 19.19.19.19 barney
  Public key for barney:
  Serial Number 05694352
  Fingerprint   309E D1DE B6DA 5145 D034

  Wait for peer to send a key[confirm]


Public key for barney:
   Serial Number 05694352
   Fingerprint   309E D1DE B6DA 5145 D034

Add this public key to the configuration? [yes/no]:yes


         Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
         Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes.
         Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
         Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes.


Mar 16 12:16:45.099: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:45.099: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:45.103: CRYPTO-KE: Received 6 bytes.
Mar 16 12:16:45.103: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:45.107: CRYPTO-KE: Received 50 bytes.
Mar 16 12:16:45.111: CRYPTO-KE: Received 14 bytes.

Send peer a key in return[confirm]
Which one?

fred? [yes]:
Public key for fred:
   Serial Number 02802219
   Fingerprint   2963 05F9 ED55 576D CF9D


         Waiting ....
         Public key for fred:
           Serial Number 02802219
         Fingerprint   2963 05F9 ED55 576D CF9D

         Add this public key to the configuration? [yes/no]:

Loser(config)#
Mar 16 12:16:55.339: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes.
Loser(config)#

Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes.
```

```
Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
Add this public key to the configuration? [yes/no]: yes
StHelen(config)#^Z
StHelen#
```

由於已經交換了公共DSS金鑰，請確保兩個路由器具有彼此的公鑰且它們匹配，如下面的命令輸出所示。

```
Loser#show crypto key mypubkey dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit

Loser#show crypto key pubkey-chain dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit

--------

StHelen#show crypto key mypubkey dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit

StHelen#show crypto key pubkey-chain dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit
```

示例1:專用鏈路的Cisco IOS配置

在每台路由器上生成DSS金鑰並交換DSS公鑰後，可以將crypto map命令應用到介面。加密會話首先生成與加密對映使用的訪問清單匹配的流量。

```
Loser#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 13:01:18 UTC Mon Mar 16 1998
! NVRAM config last updated at 13:03:02 UTC Mon Mar 16 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
crypto map oldstyle 10
 set peer barney
 match address 133
!
```

```
crypto key pubkey-chain dss
 named-key barney
  serial-number 05694352
  key-string
   B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
   732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
  quit
!
interface Ethernet0
 ip address 40.40.40.41 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 ip address 18.18.18.18 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 shutdown
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 clockrate 2400
 no cdp enable
 crypto map oldstyle
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 19.19.19.20
access-list 133 permit ip 40.40.40.0 0.0.0.255 30.30.30.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#
--------------------------

StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 13:03:05 UTC Mon Mar 16 1998
! NVRAM config last updated at 13:03:07 UTC Mon Mar 16 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
```

```
no ip domain-lookup
crypto map oldstyle 10
 set peer fred
 match address 144
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
   C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
  quit
 !
 !
interface Ethernet0
 ip address 30.30.30.31 255.255.255.0
!
interface Ethernet1
 no ip address
 shutdown
!
interface Serial0
 no ip address
 encapsulation x25
 no ip mroute-cache
 shutdown
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 compress stac
 no cdp enable
 crypto map oldstyle
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 19.19.19.19
access-list 144 permit ip 30.30.30.0 0.0.0.255 40.40.40.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#
```

示例2:適用於多點訊框中繼的Cisco IOS組態

以下命令輸出示例來自HUB路由器。

```
Loser#write terminal
Building configuration...

Current configuration:
!
```

```
! Last configuration change at 10:45:20 UTC Wed Mar 11 1998
! NVRAM config last updated at 18:28:27 UTC Tue Mar 10 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
!
crypto map oldstuff 10
 set peer barney
 match address 133
crypto map oldstuff 20
 set peer wilma
 match address 144
!
crypto key pubkey-chain dss
 named-key barney
  serial-number 05694352
  key-string
   1D460DC3 BDC73312 93B7E220 1861D55C E00DA5D8 DB2B04CD FABD297C 899D40E7
   D284F07D 6EEC83B8 E3676EC2 D813F7C8 F532DC7F 0A9913E7 8A6CB7E9 BE18790D
  quit
 named-key wilma
  serial-number 01496536
  key-string
   C26CB3DD 2A56DD50 CC2116C9 2697CE93 6DBFD824 1889F791 9BF36E70 7B29279C
   E343C56F 32266443 989B4528 1CF32C2D 9E3F2447 A5DBE054 879487F6 26A55939
  quit
!
crypto cisco pregen-dh-pairs 5
!
crypto cisco key-timeout 1440
!
interface Ethernet0
 ip address 190.190.190.190 255.255.255.0
 no ip mroute-cache
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation frame-relay
 no ip mroute-cache
 clockrate 500000
 crypto map oldstuff
!
!
ip default-gateway 10.11.19.254
ip classless
ip route 200.200.200.0 255.255.255.0 19.19.19.20
ip route 210.210.210.0 255.255.255.0 19.19.19.21
access-list 133 permit ip 190.190.190.0 0.0.0.255 200.200.200.0 0.0.0.255
access-list 144 permit ip 190.190.190.0 0.0.0.255 210.210.210.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
```

```
 password ww
 login
!
end

Loser#
```

以下命令輸出示例來自遠端站點A。

```
WAN-2511a#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
!
hostname WAN-2511a
!
enable password ww
!
no ip domain-lookup
!
crypto map mymap 10
 set peer fred
 match address 133
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D
   D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
  quit
!
interface Ethernet0
 ip address 210.210.210.210 255.255.255.0
 shutdown
!
interface Serial0
 ip address 19.19.19.21 255.255.255.0
 encapsulation frame-relay
 no fair-queue
 crypto map mymap
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 133 permit ip 210.210.210.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line 1
 no exec
 transport input all
line 2 16
 no exec
line aux 0
line vty 0 4
 password ww
 login
!
end
```

WAN-2511a#

以下命令輸出示例來自遠端站點B。

```
StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 19:00:34 UTC Tue Mar 10 1998
! NVRAM config last updated at 18:48:39 UTC Tue Mar 10 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map wabba 10
 set peer fred
 match address 144
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D
   D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
  quit
!
interface Ethernet0
 ip address 200.200.200.200 255.255.255.0
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation frame-relay
 no ip mroute-cache
 crypto map wabba
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 144 permit ip 200.200.200.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#
```

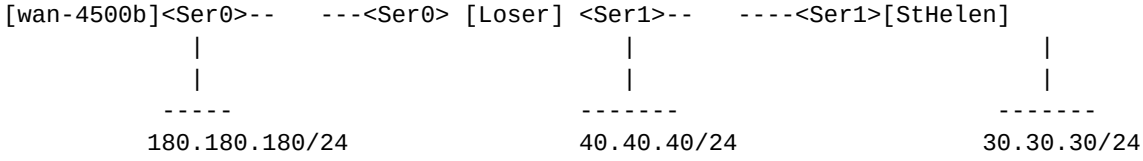
以下命令輸出示例取自幀中繼交換機。

```
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname wan-4700a
!
enable password ww
!
no ip domain-lookup
frame-relay switching
!
interface Serial0
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 100
!
interface Serial1
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 100 interface Serial0 200
 frame-relay route 300 interface Serial2 200
!
interface Serial2
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 300
!
```

示例3:對路由器進行加密

對等路由器不必相距一跳。您可以與遠端路由器建立對等作業階段。在以下示例中，目標是加密180.180.180.0/24和40.40.40.0/24之間以及180.180.180.0/24和30.30.30.0/24之間的所有網路流量。加密40.40.40.0/24和30.30.30.0/24之間的流量時沒有問題。

路由器wan-4500b與Loser和StHelen具有加密會話關聯。通過對從wan-4500b的乙太網段到StHelen的乙太網段的流量進行加密，可以避免在Loser中執行不必要的解密步驟。失敗者只需將加密流量傳送到StHelen的串列介面，然後進行解密。這會減少路由器Loader上IP封包和CPU週期的流量延遲。更重要的是，它極大地提高了系統的安全性，因為在Loser中竊聽者無法讀取流量。如果失敗者正在解密流量，則解密的資料可能會被轉移。




```
wan-4500b#write terminal
Building configuration...
```

```
Current configuration:
!
version 11.3
no service password-encryption
!
hostname wan-4500b
!
enable password 7 111E0E
!
username cse password 0 ww
no ip domain-lookup
!
crypto map toworld 10
 set peer loser
 match address 133
crypto map toworld 20
 set peer sthelen
 match address 144
!
crypto key pubkey-chain dss
 named-key loser
  serial-number 02802219
  key-string
   F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
   6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
  quit
 named-key sthelen
  serial-number 05694352
  key-string
   5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
   A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
  quit
 !
interface Ethernet0
 ip address 180.180.180.180 255.255.255.0
!
interface Serial0
 ip address 18.18.18.19 255.255.255.0
 encapsulation ppp
 crypto map toworld
!
router rip
 network 18.0.0.0
 network 180.180.0.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.31
ip route 171.68.118.0 255.255.255.0 10.11.19.254
access-list 133 permit ip 180.180.180.0 0.0.0.255 40.40.40.0 0.0.0.255
access-list 144 permit ip 180.180.180.0 0.0.0.255 30.30.30.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 password 7 044C1C
line vty 0 4
 login local
!
end

wan-4500b#

--------------------
```

```
Loser#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 11:01:54 UTC Wed Mar 18 1998
! NVRAM config last updated at 11:09:59 UTC Wed Mar 18 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
ip host StHelen.cisco.com 19.19.19.20
ip domain-name cisco.com
!
crypto map towan 10
 set peer wan
 match address 133
!
crypto key pubkey-chain dss
 named-key wan
  serial-number 07365004
  key-string
   A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
   2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
  quit
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 ip address 18.18.18.18 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 clockrate 64000
 crypto map towan
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 priority-group 1
 clockrate 64000
!
!
router rip
 network 19.0.0.0
 network 18.0.0.0
 network 40.0.0.0
!
ip default-gateway 10.11.19.254
ip classless
access-list 133 permit ip 40.40.40.0 0.0.0.255 180.180.180.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
```

```
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#

-------------------------

StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 11:13:18 UTC Wed Mar 18 1998
! NVRAM config last updated at 11:21:30 UTC Wed Mar 18 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map towan 10
 set peer wan
 match address 144
!
crypto key pubkey-chain dss
 named-key wan
  serial-number 07365004
  key-string
   A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
   2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
  quit
!
interface Ethernet0
 no ip address
!
interface Ethernet1
 ip address 30.30.30.30 255.255.255.0
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 crypto map towan
!
router rip
 network 30.0.0.0
 network 19.0.0.0
!
ip default-gateway 10.11.19.254
ip classless
```

```
access-list 144 permit ip 30.30.30.0 0.0.0.255 180.180.180.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#

--------------------------

wan-4500b#show crypto cisco algorithms
  des cfb-64
  40-bit-des cfb-64

wan-4500b#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

wan-4500b#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 0

wan-4500b#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         18.18.18.19 set    DES_56_CFB64    1683     1682
 5    Serial0         18.18.18.19 set    DES_56_CFB64    1693     1693

wan-4500b#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial0              18.18.18.19   52
wan-4500b#show crypto engine configuration
slot:               0
engine name:        wan
engine type:        software
serial number:      07365004
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    303
input queue bot:    303
input queue count:  0

wan-4500b#show crypto key mypubkey dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

wan-4500b#show crypto key pubkey-chain dss
crypto public-key loser 02802219
 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
quit
crypto public-key sthelen 05694352
 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
quit
```

```
wan-4500b#show crypto map interface serial 1
No crypto maps found.

wan-4500b#show crypto map
Crypto Map "toworld" 10 cisco
        Connection Id = 1        (1 established,    0 failed)
        Peer = loser
        PE = 180.180.180.0
        UPE = 40.40.40.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 180.180.180.0/0.0.0.255
                dest:   addr = 40.40.40.0/0.0.0.255

Crypto Map "toworld" 20 cisco
        Connection Id = 5        (1 established,    0 failed)
        Peer = sthelen
        PE = 180.180.180.0
        UPE = 30.30.30.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 180.180.180.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255

wan-4500b#

--------------------------

Loser#show crypto cisco algorithms
  des cfb-64
  des cfb-8
  40-bit-des cfb-64
  40-bit-des cfb-8

Loser#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10

Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 61   Serial0         18.18.18.18 set    DES_56_CFB64    1683     1682

Loser#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial0              18.18.18.18   1
Serial1              19.19.19.19   90
Loser#show crypto engine configuration
slot:               0
engine name:        loser
engine type:        software
serial number:      02802219
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    235
input queue bot:    235
input queue count:  0

Loser#show crypto key mypubkey dss
crypto public-key loser 02802219
```

```
 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
quit

Loser#show crypto key pubkey-chain dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

Loser#show crypto map interface serial 1
No crypto maps found.

Loser#show crypto map
Crypto Map "towan" 10 cisco
        Connection Id = 61       (0 established,    0 failed)
        Peer = wan
        PE = 40.40.40.0
        UPE = 180.180.180.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

Loser#

----------------------------------------

StHelen#show crypto cisco algorithms
  des cfb-64

StHelen#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

StHelen#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10

StHelen#show crypto engine connections active

ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 58   Serial1         19.19.19.20 set    DES_56_CFB64    1694     1693

StHelen#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Ethernet0            0.0.0.0       1
Serial1              19.19.19.20   80
StHelen#show crypto engine configuration
slot:               0
engine name:        sthelen
engine type:        software
serial number:      05694352
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    220
input queue bot:    220
input queue count:  0

StHelen#show crypto key mypubkey dss
crypto public-key sthelen 05694352
 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
```

```
quit

StHelen#show crypto key pubkey-chain dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

StHelen#show crypto map interface serial 1
Crypto Map "towan" 10 cisco
        Connection Id = 58       (1 established,    0 failed)
        Peer = wan
        PE = 30.30.30.0
        UPE = 180.180.180.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 30.30.30.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

StHelen#show crypto map
Crypto Map "towan" 10 cisco
        Connection Id = 58       (1 established,    0 failed)
        Peer = wan
        PE = 30.30.30.0
        UPE = 180.180.180.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 30.30.30.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

StHelen#
```

示例4:使用DDR進行加密

因為Cisco IOS依賴ICMP建立加密會話，所以通過DDR鏈路進行加密時，ICMP流量在撥號程式清單中必須分類為「感興趣」。

注意：壓縮在Cisco IOS軟體版本11.3中有效，但對於加密資料不是很實用。因為加密的資料看起來相當隨機，所以壓縮只會減慢速度。但是您可以針對非加密流量開啟此功能。

在某些情況下，您需要將撥號備份連線到同一路由器。例如，當使用者希望防止其WAN網路中的特定鏈路發生故障時，它就非常有用。如果兩個介面轉到同一個對等體，則可以在兩個介面上使用相同的加密對映。必須使用備份介面才能使此功能正常工作。如果備份設計中有一個路由器撥入另一個裝置，則應建立不同的加密對映並相應地設定對等體。同樣地，應使用**backup interface**命令。

```
dial-5#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname dial-5
!
boot system c1600-sy56-l 171.68.118.83
enable secret 5 $1$oNe1wDbhBdcN6x9Y5gfuMjqh10
!
```

```
username dial-6 password 0 cisco
isdn switch-type basic-ni1
!
crypto map dial6 10
 set peer dial6
 match address 133
!
crypto key pubkey-chain dss
 named-key dial6
  serial-number 05679987
  key-string
   753F71AB E5305AD4 3FCDFB6D 47AA2BB5 656BFCAA 53DBE37F 07465189 06E91A82
   2BC91236 13DC4AA8 7EC5B48C D276E5FE 0D093014 6D3061C5 03158820 B609CA7C
  quit
!
interface Ethernet0
 ip address 20.20.20.20 255.255.255.0
!
interface BRI0
 ip address 10.10.10.11 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 dialer idle-timeout 9000
 dialer map ip 10.10.10.10 name dial-6 4724118
 dialer hold-queue 40
 dialer-group 1
 isdn spid1 919472417100 4724171
 isdn spid2 919472417201 4724172
 compress stac
 ppp authentication chap
 ppp multilink
 crypto map dial6
!
ip classless
ip route 40.40.40.0 255.255.255.0 10.10.10.10
access-list 133 permit ip 20.20.20.0 0.0.0.255 40.40.40.0 0.0.0.255
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password ww
 login
!
end

dial-5#

-----------------------

dial-6#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname dial-6
!
boot system c1600-sy56-l 171.68.118.83
```

```
enable secret 5 $1$VdPYuA/BIVeEm9UAFEm.PPJFc.
!
username dial-5 password 0 cisco
no ip domain-lookup
isdn switch-type basic-ni1
!
 crypto map dial5 10
 set peer dial5
 match address 144
!
crypto key pubkey-chain dss
 named-key dial5
  serial-number 05679919
  key-string
   160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F
   F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145
  quit
 !
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
!
interface BRI0
 ip address 10.10.10.10 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 dialer idle-timeout 9000
 dialer map ip 10.10.10.11 name dial-5 4724171
 dialer hold-queue 40
 dialer load-threshold 5 outbound
 dialer-group 1
 isdn spid1 919472411800 4724118
 isdn spid2 919472411901 4724119
 compress stac
 ppp authentication chap
 ppp multilink
 crypto map dial5
!
ip classless
ip route 20.20.20.0 255.255.255.0 10.10.10.11
access-list 144 permit ip 40.40.40.0 0.0.0.255 20.20.20.0 0.0.0.255
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password ww
 login
!
end

dial-6#
```

示例5:加密IP隧道中的IPX流量

在此範例中，IP通道中的IPX流量會進行加密。

注意：僅加密此通道(IPX)中的流量。所有其他IP流量都處於閒置狀態。

```
WAN-2511a#write terminal
Building configuration...
```

```
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname WAN-2511a
!
enable password ww
!
no ip domain-lookup
ipx routing 0000.0c34.aa6a
!
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
 quit
!
crypto map wan2516 10
 set peer wan2516
 match address 133
!
!
interface Loopback1
 ip address 50.50.50.50 255.255.255.0
!
interface Tunnel1
 no ip address
 ipx network 100
 tunnel source 50.50.50.50
 tunnel destination 60.60.60.60
 crypto map wan2516
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
 ipx network 600
!
interface Serial0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 crypto map wan2516
!
interface Serial1
 no ip address
 shutdown
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit ip host 50.50.50.50 host 60.60.60.60
!
line con 0
 exec-timeout 0 0
 password ww
 login
line 1 16
line aux 0
 password ww
 login
line vty 0 4
 password ww
 login
```

```
!
end

WAN-2511a#

------------------------

WAN-2516a#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname WAN-2516a
!
enable password ww
!
no ip domain-lookup
ipx routing 0000.0c3b.cc1e
!
crypto public-key wan2511 01496536
 C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D
 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553
 quit
!
crypto map wan2511 10
 set peer wan2511
 match address 144
!
!
hub ether 0 1
 link-test
 auto-polarity
!
! <other hub interfaces snipped>
!
hub ether 0 14
 link-test
 auto-polarity
!
interface Loopback1
 ip address 60.60.60.60 255.255.255.0
!
interface Tunnel1
 no ip address
 ipx network 100
 tunnel source 60.60.60.60
 tunnel destination 50.50.50.50
 crypto map wan2511
!
interface Ethernet0
 ip address 30.30.30.30 255.255.255.0
 ipx network 400
!
interface Serial0
 ip address 20.20.20.20 255.255.255.0
 encapsulation ppp
 clockrate 2000000
 crypto map wan2511
```

```
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
!
ip default-gateway 20.20.20.21
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.21
access-list 144 permit ip host 60.60.60.60 host 50.50.50.50
access-list 188 permit gre any any
!
line con 0
 exec-timeout 0 0
 password ww
 login
line aux 0
 password ww
 login
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end

WAN-2516a#
-----------------------

WAN-2511a#show ipx route
Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses

3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C        100 (TUNNEL),        Tu1
C        600 (NOVELL-ETHER),  Et0
R        400 [151/01] via      100.0000.0c3b.cc1e,   24s, Tu1


WAN-2511a#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    207      207


WAN-2511a#ping 400.0000.0c3b.cc1e
Translating "400.0000.0c3b.cc1e"

Type escape sequence to abort.
Sending 5, 100-byte IPX cisco Echoes to 400.0000.0c3b.cc1e, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/48 ms


WAN-2511a#show crypto engine connections active
```

```
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    212      212


WAN-2511a#ping 30.30.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms


WAN-2511a#show crypto engine connections active

ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    212      212

WAN-2511a#
```

示例6:加密L2F通道

在此範例中，只嘗試加密撥入使用者的L2F流量。此處，「user@cisco.com」呼叫其所在城市中名為「DEMO2」的本地網路訪問伺服器(NAS)，並通過隧道連線到家庭網關CD。所有DEMO2流量（以及其他L2F呼叫者的流量）均經過加密。因為L2F使用UDP埠1701，所以這就是訪問清單的構建方式，用於確定加密哪些流量。

注意：如果尚未設定加密關聯（表示呼叫者是第一個呼叫並建立L2F隧道的人），則呼叫者可能會由於設定加密關聯延遲而被丟棄。具有足夠CPU電源的路由器可能不會發生這種情況。此外，您可能希望增加**keytimeout**，以便僅在非高峰時間進行加密設定和拆除。

以下命令輸出示例是從遠端NAS獲取的。

```
DEMO2#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname DEMO2
!
enable password ww
!
username NAS1 password 0 SECRET
username HomeGateway password 0 SECRET
no ip domain-lookup
vpdn enable
vpdn outgoing cisco.com NAS1 ip 20.20.20.20
!
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
 quit
!
crypto map vpdn 10
 set peer wan2516
 match address 133
```

```
!
crypto key-timeout 1440
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
!
interface Serial0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 crypto map vpdn
!
interface Serial1
 no ip address
 shutdown
!
interface Group-Async1
 no ip address
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 no cdp enable
 ppp authentication chap pap
 group-range 1 16
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit udp host 20.20.20.21 eq 1701
 host 20.20.20.20 eq 1701
!
!
line con 0
 exec-timeout 0 0
 password ww
 login
line 1 16
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware
line aux 0
 login local
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end

DEMO2#
```

以下命令輸出示例是從家庭網關獲取的。

```
CD#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service pad
```

```
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname CD
!
enable password ww
!
username NAS1 password 0 SECRET
username HomeGateway password 0 SECRET
username user@cisco.com password 0 cisco
no ip domain-lookup
vpdn enable
vpdn incoming NAS1 HomeGateway virtual-template 1
!
crypto public-key wan2511 01496536
 C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D
 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553
 quit
!
crypto key-timeout 1440
!
crypto map vpdn 10
 set peer wan2511
 match address 144
!
!
hub ether 0 1
 link-test
 auto-polarity
!
interface Loopback0
 ip address 70.70.70.1 255.255.255.0
!
interface Ethernet0
 ip address 30.30.30.30 255.255.255.0
!
interface Virtual-Template1
 ip unnumbered Loopback0
 no ip mroute-cache
 peer default ip address pool default
 ppp authentication chap
!
interface Serial0
 ip address 20.20.20.20 255.255.255.0
 encapsulation ppp
 clockrate 2000000
 crypto map vpdn
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
!
ip local pool default 70.70.70.2 70.70.70.77
ip default-gateway 20.20.20.21
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.21
access-list 144 permit udp host 20.20.20.20 eq 1701 host 20.20.20.21 eq 1701
!
line con 0
```

```
 exec-timeout 0 0
 password ww
 login
line aux 0
 password ww
 login
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end
```

疑難排解

通常，最好通過使用以下**show**命令收集資訊來開始每個故障排除會話。星號(*)表示命令特別有用。另請參閱IP安全性疑難排解 — 瞭解和使用debug命令以瞭解其他資訊。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

注意：發出debug指令之前，請先參閱有關Debug指令的重要資訊。

指令	
show crypto cisco algorithms	show crypto cisco key-timeout
show crypto cisco pregen-dh-pairs	* show crypto engine connections active
show crypto engine connections dropped-packet	show crypto engine configuration
show crypto key mypubkey dss	* show crypto key pubkey-chain dss
show crypto map interface serial 1	* show crypto map
debug crypto engine	* debug crypto sess
debug cry key	clear crypto connection
加密歸零	no crypto public-key

- **show crypto cisco algorithms**— 必須啟用所有用於與任何其他對等加密路由器通訊的資料加密標準(DES)演算法。如果不啟用DES演算法，則將無法使用該演算法，即使您以後嘗試將該演算法分配給**加密對映**。如果您的路由器嘗試與對等路由器建立加密通訊會話，並且兩台路由器兩端未啟用相同的DES演算法，則加密會話將失敗。如果兩端至少啟用了一個通用DES演算法，則加密會話可以繼續。**注意：**Cisco IOS軟體版本11.3中會顯示額外的單詞cisco，需要它來區分Cisco IOS軟體版本11.2中的IPSec和Cisco專有加密。

```
Loser#show crypto cisco algorithms
  des cfb-64
  des cfb-8
  40-bit-des cfb-64
  40-bit-des cfb-8
```

- **show crypto cisco key-timeout** — 加密的通訊會話建立後，它在特定時間長度內有效。經過此時間之後，會話超時。必須協商新的會話，並且必須生成新的DES（會話）金鑰才能繼續加密通訊。使用此命令可以更改加密通訊會話在過期之前持續的時間（超時）。

```
Loser#show crypto cisco key-timeout
```

```
Session keys will be re-negotiated every 30 minutes
```

使用這些命令確定DES金鑰重新協商之前的時間長度。

```
StHelen#show crypto conn
Connection Table
PE              UPE         Conn_id New_id Algorithm    Time
0.0.0.1         0.0.0.1        4    0      DES_56_CFB64 Mar 01 1993 03:16:09
                flags:TIME_KEYS


StHelen#show crypto key
Session keys will be re-negotiated every 30 minutes

StHelen#show clock
*03:21:23.031 UTC Mon Mar 1 1993
```

- **show crypto cisco pregen-dh-pairs** — 每個加密會話使用唯一的DH編號對。每次建立新會話時，必須生成新的DH號碼對。會話完成後，這些數字將被丟棄。生成新的DH編號對是CPU密集型活動，這會導致會話設定緩慢，尤其是對於低端路由器。要加速會話設定，可以選擇預生成指定數量的DH編號對並將其保留為保留狀態。然後，當建立加密通訊會話時，從該保留區提供DH號碼對。在使用DH號碼對之後，用新的DH號碼對自動補充該保留，以便始終有一個可用的DH號碼對。通常無需預先產生多個或兩個DH編號對，除非您的路由器經常設定多個加密會話，導致預先產生的一或兩個DH編號對保留資源耗盡得太快。

```
Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10
```

- **show crypto cisco connections active**以下是命令輸出示例。

```
Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 16   Serial1         19.19.19.19 set    DES_56_CFB64    376      884
```

- **show crypto cisco engine connections dropped-packet**以下是命令輸出示例。

```
Loser#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial1              19.19.19.19   39
```

- **show crypto engine configuration**(在Cisco IOS軟體版本11.2中為**show crypto engine brief。**)以下是命令輸出示例。

```
Loser#show crypto engine configuration
slot:               0
engine name:        fred
engine type:        software
serial number:      02802219
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    465
input queue bot:    465
input queue count:  0
```

- **show crypto key mypubkey dss**以下是命令輸出示例。

```
Loser#show crypto key mypubkey dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit
```

- **show crypto key pubkey-chain dss**以下是命令輸出示例。

```
Loser#show crypto key pubkey-chain dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit
```

- **show crypto map interface serial 1**以下是命令輸出示例。

```
Loser#show crypto map interface serial 1
Crypto Map "oldstyle" 10 cisco
        Connection Id = 16       (8 established,    0 failed)
        Peer = barney
        PE = 40.40.40.0
        UPE = 30.30.30.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255
```

使用ping命令時請注意時間差異。

```
wan-5200b#ping 30.30.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms
wan-5200b#
-----------
wan-5200b#ping 30.30.30.31

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.31, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms
-----------------

wan-5200b#ping 19.19.19.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24 ms
------------
```

- show crypto map interface serial 1以下是命令輸出示例。

```
Loser#show crypto map
Crypto Map "oldstyle" 10 cisco
        Connection Id = 16       (8 established,    0 failed)
        Peer = barney
        PE = 40.40.40.0
        UPE = 30.30.30.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255
```

- debug crypto engine以下是命令輸出示例。

```
Loser#debug crypto engine
Mar 17 11:49:07.902: Crypto engine 0: generate alg param

Mar 17 11:49:07.906: CRYPTO_ENGINE: Dh phase 1 status: 0
Mar 17 11:49:07.910: Crypto engine 0: sign message using crypto engine
Mar 17 11:49:09.894: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:11.758: Crypto engine 0: generate alg param

Mar 17 11:49:12.246: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:13.342: CRYPTO ENGINE 0: get syndrome for conn id 25
Mar 17 11:49:13.346: Crypto engine 0: verify signature
Mar 17 11:49:14.054: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:14.402: Crypto engine 0: sign message using crypto engine
Mar 17 11:49:14.934: Crypto engine 0: create session for conn id 25
Mar 17 11:49:14.942: CRYPTO ENGINE 0: clear dh number for conn id 25
Mar 17 11:49:24.946: Crypto engine 0: generate alg param
```

- **debug crypto sessmgmt**以下是命令輸出示例。

```
StHelen#debug crypto sessmgmt

Mar 17 11:49:08.918: IP: s=40.40.40.40 (Serial1), d=30.30.30.30, len 328,
              Found an ICMP connection message.

Mar 17 11:49:08.922: CRYPTO: Dequeued a message: CIM
Mar 17 11:49:08.926: CRYPTO-SDU: Key Timeout, Re-exchange Crypto Keys
Mar 17 11:49:09.978: CRYPTO: Verify done. Status=OK
Mar 17 11:49:09.994: CRYPTO: DH gen phase 1 status for conn_id 22 slot 0:OK
Mar 17 11:49:11.594: CRYPTO: DH gen phase 2 status for conn_id 22 slot 0:OK
Mar 17 11:49:11.598: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
Mar 17 11:49:12.134: CRYPTO: Sign done. Status=OK
Mar 17 11:49:12.142: CRYPTO: ICMP message sent: s=19.19.19.20, d=19.19.19.19
Mar 17 11:49:12.146: CRYPTO-SDU: act_on_nnc_req: NNC Echo Reply sent
Mar 17 11:49:12.154: CRYPTO: Create encryption key for conn_id 22 slot 0:OK
Mar 17 11:49:15.366: CRYPTO: Dequeued a message: CCM
Mar 17 11:49:15.370: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
Mar 17 11:49:16.430: CRYPTO: Verify done. Status=OK
Mar 17 11:49:16.434: CRYPTO: Replacing -23 in crypto maps with 22 (slot 0)
Mar 17 11:49:26.438: CRYPTO: Need to pregenerate 1 pairs for slot 0.
Mar 17 11:49:26.438: CRYPTO: Pregenerating DH for conn_id 32 slot 0
Mar 17 11:49:28.050: CRYPTO: DH phase 1 status for conn_id 32 slot 0:OK
                           ~~ <---------- This is good ----------> ~~
```

如果在加密對映上設定了錯誤的對等體，則會收到此錯誤消息。

```
Mar  2 12:19:12.639: CRYPTO-SDU:Far end authentication error:
          Connection message verify failed
```

如果加密演算法不匹配，您將收到此錯誤消息。

```
Mar  2 12:26:51.091: CRYPTO-SDU: Connection
failed due to incompatible policy
```

如果DSS金鑰丟失或無效，您將收到此錯誤消息。

```
Mar 16 13:33:15.703: CRYPTO-SDU:Far end authentication error:
           Connection message verify failed
```

- **debug crypto key**以下是命令輸出示例。

```
StHelen#debug crypto key
Mar 16 12:16:45.795: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:45.795: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:45.799: CRYPTO-KE: Sent 6 bytes.
Mar 16 12:16:45.799: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:45.803: CRYPTO-KE: Sent 64 bytes.

Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes.
Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
```

- **clear crypto connection**以下是命令輸出示例。

```
wan-2511#show crypto engine connections act
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 9    Serial0         20.20.20.21 set    DES_56_CFB64    29       28

wan-2511#clear crypto connection 9
wan-2511#
*Mar  5 04:58:20.690: CRYPTO: Replacing 9 in crypto maps with 0 (slot 0)
*Mar  5 04:58:20.694: Crypto engine 0: delete connection 9
*Mar  5 04:58:20.694: CRYPTO: Crypto Engine clear conn_id 9 slot 0: OK
wan-2511#
wan-2511#show crypto engine connections act
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt

wan-2511#
```

- **加密歸零**以下是命令輸出示例。

```
wan-2511#show crypto mypubkey
crypto public-key wan2511 01496536
 11F43C02 70C0ADB7 5DD50600 A0219E04 C867A5AF C40A4FE5 CE99CCAB A8ECA840
 EB95FBEE D727ED5B F0A6F042 BDB5529B DBB0698D DB0B2756 F6CABE8F 05E4B27F
quit

wan-2511#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wan-2511(config)#crypto zeroize
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named wan2511.
Do you really want to remove these keys? [yes/no]: yes
% Zeroize done.

wan-2511(config)#^Z
wan-2511#
wan-2511#show crypto mypubkey
wan-2511#
```

- no crypto public-key以下是命令輸出示例。

```
wan-2511#show crypto pubkey
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
quit

wan-2511#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wan-2511(config)#crypto public-key ?
  WORD  Peer name

wan-2511(config)#
wan-2511(config)#no crypto public-key wan2516 01698232
wan-2511(config)#^Z
wan-2511#
wan-2511#show crypto pubkey
wan-2511#
```

使用ESA排除Cisco 7200故障

思科還提供硬體協助選項，用於在稱為ESA的Cisco 7200系列路由器上進行加密。ESA的形式為VIP2-40卡的埠介面卡或Cisco 7200的獨立埠介面卡。這種配置允許使用硬體介面卡或VIP2軟體引擎對通過Cisco 7500 VIP2卡上的介面傳入或傳出的資料進行加密和解密。Cisco 7200允許硬體協助加密Cisco 7200機箱上任何介面的流量。使用加密協助可節省寶貴的CPU週期，這些週期可用於其它用途，例如路由或任何其他Cisco IOS功能。

在Cisco 7200上，獨立連線埠配接器的設定與Cisco IOS軟體加密引擎完全相同，但有一些額外命令，僅用於硬體和決定哪個引擎（軟體或硬體）進行加密。

首先，準備路由器以進行硬體加密：

```
wan-7206a(config)#
%OIR-6-REMCARD: Card removed from slot 3, interfaces disabled
*Mar  2 08:17:16.739: ...switching to SW crypto engine

wan-7206a#show crypto card 3
```

```
Crypto card in slot: 3

Tampered:        No
Xtracted:        Yes
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
wan-7206a#

wan-7206a(config)#

wan-7206a(config)#crypto zeroize 3
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named hard.
Do you really want to remove these keys? [yes/no]: yes
[OK]
```

啟用或禁用硬體加密，如下所示：

```
wan-7206a(config)#crypto esa shutdown 3
...switching to SW crypto engine


wan-7206a(config)#crypto esa enable 3
There are no keys on the ESA in slot 3- ESA not enabled.
```

接下來，在啟用ESA之前為其生成金鑰。

```
wan-7206a(config)#crypto gen-signature-keys hard
% Initialize the crypto card password. You will need
   this password in order to generate new signature
   keys or clear the crypto card extraction latch.

Password:
Re-enter password:
Generating DSS keys ....
 [OK]

wan-7206a(config)#
wan-7206a#show crypto mypubkey
crypto public-key hard 00000052
 EE691A1F BD013874 5BA26DC4 91F17595 C8C06F4E F7F736F1 AD0CACEC 74AB8905
 DF426171 29257F8E B26D49B3 A8E11FB0 A3501B13 D3F19623 DCCE7322 3D97B804
quit

wan-7206a#
wan-7206a(config)#crypto esa enable 3
...switching to HW crypto engine

wan-7206a#show crypto engine brie
crypto engine name:   hard
crypto engine type:   ESA
serial number:        00000052
crypto engine state:  installed
crypto firmware version:  5049702
crypto engine in slot: 3

wan-7206a#
```

使用ESA排除VIP2故障

VIP2卡上的ESA硬體埠介面卡用於對通過VIP2卡上的介面傳入或傳出的資料進行加密和解密。與Cisco 7200一樣，使用加密幫助可節省寶貴的CPU週期。在這種情況下，**crypto esa enable**命令不存在，因為ESA埠介面卡對VIP2卡上的埠進行加密（如果ESA已插入）。如果ESA埠介面卡是首次安裝，或者卸下，然後重新安裝，則需要將**crypto clear-latch**應用於該插槽。

```
Router#show crypto card 11

Crypto card in slot: 11

Tampered:        No
Xtracted:        Yes
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
Router#
```

由於提取了ESA加密模組，因此在該插槽上執行**crypto clear-latch**命令之前，您將收到以下錯誤消息，如下所示。

```
----
*Jan 24 02:57:09.583: CRYPTO: Sign done. Status= Extraction latch set. Request not allowed.
-----
Router(config)#crypto clear-latch ?
  <0-15>  Chassis slot number

Router(config)#crypto clear-latch 11
% Enter the crypto card password.
Password:
Router(config)#^Z
```

如果您忘記了以前分配的密碼，請使用**crypto zeroize**命令而不是**crypto clear-latch**命令重置ESA。發出**crypto zeroize**命令後，必須重新生成並重新交換DSS金鑰。重新生成DSS金鑰時，系統會提示您建立新密碼。示例如下。

```
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show crypto card 11

Crypto card in slot: 11

Tampered:        No
Xtracted:        No
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
Router#

-------------------------------------------------


Router#show crypto engine brief
crypto engine name:   TERT
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  dss key generated
crypto lib version:   5.0.0
crypto engine in slot: 6
```

```
crypto engine name:   WAAA
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  dss key generated
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
-----------
Router(config)#crypto zeroize
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named TERT.
Do you really want to remove these keys? [yes/no]: yes
% Zeroize done.

Router(config)#crypto zeroize  11
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named WAAA.
Do you really want to remove these keys? [yes/no]: yes
[OK]

Router(config)#^Z
Router#show crypto engine brief
crypto engine name:   unknown
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  installed
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   unknown
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  installed
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
--------------
Router(config)#crypto gen-signature-keys VIPESA 11
% Initialize the crypto card password. You will need
   this password in order to generate new signature
   keys or clear the crypto card extraction latch.

Password:
Re-enter password:
Generating DSS keys ....
 [OK]

Router(config)#
*Jan 24 01:39:52.923: Crypto engine 11: create key pairs.
^Z
Router#
------
Router#show crypto engine brief
crypto engine name:   unknown
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  installed
crypto lib version:   5.0.0
crypto engine in slot: 6
```

```
crypto engine name:   VIPESA
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  dss key generated
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
----------
Router#show crypto engine connections active 11
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 2    Serial11/0/0    20.20.20.21 set    DES_56_CFB64    9996     9996

Router#
Router#clear crypto connection 2 11
Router#
*Jan 24 01:41:04.611: CRYPTO: Replacing 2 in crypto maps with 0 (slot 11)
*Jan 24 01:41:04.611: Crypto engine 11: delete connection 2
*Jan 24 01:41:04.611: CRYPTO: Crypto Engine clear conn_id 2 slot 11: OK
Router#show crypto engine connections active 11
No connections.

Router#
*Jan 24 01:41:29.355: CRYPTO ENGINE:Number of connection entries
received from VIP 0
------------

Router#show crypto mypub
% Key for slot 11:
crypto public-key VIPESA 00000078
 CF33BA60 56FCEE01 2D4E32A2 5D7ADE70 6AF361EE 2964F3ED A7CE08BD A87BF7FE
 90A39F1C DF96143A 9B7B9C78 5F59445C 27860F1E 4CD92B6C FBC4CBCC 32D64508
quit

Router#show crypto pub
crypto public-key wan2516 01698232
 C5DE8C46 8A69932C 70C92A2C 729449B3 FD10AC4D 1773A997 7F6BA37D 61997AC3
 DBEDBEA7 51BF3ADD 2BB35CB5 B9126B4D 13ACF93E 0DF0CD22 CFAAC1A8 9CE82985
quit

Router#
----------
interface Serial11/0/0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 ip route-cache distributed
 no fair-queue
 no cdp enable
 crypto map test
!
----------
Router#show crypto eng conn act 11
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 3    Serial11/0/0    20.20.20.21 set    DES_56_CFB64    761      760

Router#
*Jan 24 01:50:43.555: CRYPTO ENGINE:Number of connection
entries received from VIP 1

Router#
```

相關資訊

- 思科網路層加密配置和故障排除：IPSec和ISAKMP — 第2部分
- 美國國家標準與技術研究所(NIST)的DES FIPS 46-2
- DSS FIPS 186 at National Institute of Standards and Technology(NIST)
- RSA Laboratories有關當今加密技術的常見問題
- IETF安全標準
- 配置Internet金鑰交換安全協定
- 配置IPSec網路安全
- IPSec支援頁面
- 技術支援 - Cisco Systems