思科網路層加密配置和故障排除：IPSec和ISAKMP — 第2部分

目錄

簡介

本技術報告的第一部分介紹了網路層加密背景資訊和基本網路層加密配置。本文此部分涵蓋IP安全(IPSec)和網際網路安全關聯和金鑰管理協定(ISAKMP)。

IPSec是在Cisco IOS®軟體版本11.3T中匯入。它提供了一種安全資料傳輸機制，由ISAKMP/Oakley和IPSec組成。

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11.3(T)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

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。

IPSec和ISAKMP

本文此部分介紹IPSec和ISAKMP。

IPSec是在Cisco IOS軟體版本11.3T中匯入。它提供了一種安全資料傳輸機制，由ISAKMP/Oakley和IPSec組成。

IPSec通訊協定

IPSec通訊協定(RFC 1825)提供IP網路層加密，並定義一組新增的標頭以新增到IP資料包。這些新報頭放置在IP報頭之後和第4層協定（通常為TCP或UDP）之前。 它們提供保護IP資料包負載的資訊，如下所述：

身份驗證報頭(AH)和封裝安全負載(ESP)可以單獨使用，也可以一起使用，儘管對於大多數應用，它們中僅有一個就足夠了。對於這兩種協定，IPSec並不定義要使用的具體安全演算法，而是為實施行業標準演算法提供了一個開放式框架。最初，大多數IPSec實現都支援RSA Data Security的MD5或美國政府定義的用於完整性和身份驗證的安全雜湊演算法(SHA)。DES是目前最常用的批次加密演算法，儘管RFC可用於定義如何使用許多其他加密系統，包括IDEA、Blowfish和RC4。

- **AH**(請參閱RFC 1826)AH是一種為IP資料包提供強完整性和身份驗證的機制。它還可以提供不可否認性，這取決於使用哪種加密演算法和執行金鑰管理。例如，使用非對稱數位簽章演算法（如RSA）可以提供不可否認性。AH不提供機密性和流量分析保護。需要保密的使用者應考慮使用IP ESP來代替AH或與AH一起使用。AH可能顯示在每個躍點處檢查的任何其他報頭之後，以及在中間躍點處未檢查的任何其他報頭之前。緊接AH前面的IPv4或IPv6報頭在其Next Header（或Protocol）欄位中包含值51。
- **ESP**(請參閱RFC 1827)ESP可以出現在IP報頭之後和最終傳輸層協定之前。Internet編號分配機構已將協定編號50分配給ESP。ESP報頭前面的報頭始終在其Next Header(IPv6)或Protocol(IPv4)欄位中包含值50。ESP由未加密報頭以及加密資料組成。加密資料包括受保護的ESP報頭欄位和受保護的使用者資料，後者是整個IP資料包或上層協定幀（如TCP或UDP）。IP ESP通過加密要保護的資料並將加密的資料放在IP ESP的資料部分來提供保密性和完整性。根據使用者安全性要求，此機制可用於加密傳輸層區段（例如TCP、UDP、ICMP、IGMP）或整個IP資料包。封裝受保護的資料對於為整個原始資料包提供機密性是必要的。使用本規範將增加參與系統的IP協定處理成本，同時也會增加通訊延遲。延遲增加主要是由於包含ESP的每個IP資料包需要加密和解密。在通道模式ESP中，原始IP資料包放在ESP的加密部分中，而整個ESP訊框放在一個具有未加密IP標頭的資料包中。未加密IP報頭中的資訊用於將安全資料包從源路由到目標。未加密的IP路由報頭可能包含在IP報頭和ESP之間。此模式允許網路裝置（例如路由器）充當IPSec代理。也就是說，路由器代表主機執行加密。來源的路由器會加密封

包並沿IPSec通道轉送這些封包。目的地的路由器解密原始IP資料包並將其轉發到目的地系統。通道模式的主要優點是終端系統不需要修改就可以享受IP安全的好處。通道模式還能防止流量分析；在通道模式下，攻擊者只能確定通道端點，而不能確定通道資料包的真正源和目標，即使它們與通道端點相同。根據IETF的定義，只有在源系統和目標系統都瞭解IPSec時，才能使用IPSec傳輸模式。在大多數情況下，您使用隧道模式部署IPSec。這樣，您就可以在網路架構中實施IPSec，而無需修改PC、伺服器和主機上的作業系統或任何應用程式。在傳輸模式ESP中，ESP報頭會緊接在傳輸層協定報頭（例如TCP、UDP或ICMP）之前插入IP資料包。在此模式下，由於沒有加密的IP報頭或IP選項，因此節省了頻寬。只有IP負載會加密，而原始IP報頭會保持不變。此模式的優點是每個資料包只新增幾個位元組。也允許公用網路上的裝置看到封包的最終來源和目的地。此功能允許您根據IP報頭上的資訊，在中間網路中啟用特殊處理（例如，服務品質）。但是，第4層報頭將被加密，從而限制對資料包的檢查。遺憾的是，通過以清除模式傳遞IP報頭，傳輸模式允許攻擊者執行一些流量分析。例如，攻擊者可以看到某位CEO向另一位CEO傳送大量資料包的時間。但是，攻擊者只知道IP資料包被傳送；攻擊者無法確定他們是電子郵件還是其他應用程式。

ISAKMP/奧克利

雖然IPSec是保護IP資料包的實際協定，但ISAKMP是協商策略的協定，並為生成IPSec對等體共用的金鑰提供一個通用框架。它沒有指定金鑰管理或金鑰交換的任何細節，並且不繫結到任何金鑰生成技術。在ISAKMP內部，思科使用Oakley作為金鑰交換協定。Oakley允許您在五個「知名」組中進行選擇。Cisco IOS支援組1（768位金鑰）和組2（1024位金鑰）。 Cisco IOS軟體版本12.1(3)T中引入對群組5（1536位元金鑰）的支援。

ISAKMP/Oakley在兩個實體之間建立經過身份驗證的安全隧道，然後協商IPSec的安全關聯。此過程要求兩個實體相互驗證自身並建立共用金鑰。

雙方必須相互驗證。ISAKMP/Oakley支援多種身份驗證方法。兩個實體必須使用RSA簽名、RSA加密金鑰或預共用金鑰通過協商過程就通用身份驗證協定達成一致。

雙方都必須具有共用作業階段金鑰才能加密ISAKMP/Oakley通道。Diffie-Hellman通訊協定用於協定共用作業階段金鑰。交換機會按照上述步驟進行身份驗證，以防止「中間人」攻擊。

身份驗證和金鑰交換這兩個步驟用於建立ISAKMP/Oakley會話關聯(SA)，這是兩台裝置之間的安全隧道。隧道的一側提供一組演算法；然後，另一端必須接受其中一個提議或拒絕整個連線。當雙方就使用哪些演算法達成一致後，他們必須推導用於IPSec的AH、ESP或兩者的關鍵材料。

IPSec使用的共用金鑰不同於ISAKMP/Oakley。可以再次使用Diffie-Hellman以確保完善的前向保密性，或者通過刷新源自原始Diffie-Hellman交換(該交換通過用偽隨機數(nonces)雜湊生成ISAKMP/Oakley SA)的共用金鑰來匯出IPSec共用金鑰。 第一種方法提供更高的安全性，但速度較慢。在大多數實現中，使用這兩種方法的組合。也就是說，Diffie-hellman用於第一次金鑰交換，然後本地策略決定何時使用Diffie-hellman或僅僅進行金鑰刷新。完成後，IPSec SA即建立。

RSA簽名和RSA加密的金鑰都需要遠端對等體的公鑰，並且它們還要求遠端對等體具有您的本地公鑰。公共金鑰以證書形式在ISAKMP中交換。這些憑證是在憑證授權單位(CA)中註冊取得。 目前，如果路由器中沒有證書，ISAKMP不會協商保護套件RSA簽名。

思科路由器不建立證書。路由器建立金鑰，並為這些金鑰請求證書。將路由器的金鑰繫結到其標識的證書由證書頒發機構建立和簽名。這是一項管理功能，證書頒發機構始終需要某種驗證以驗證使用者是否是其所聲稱的使用者。這表示您不能即時建立新證書。

通訊機器交換它們從證書頒發機構獲得的預先存在的證書。證書本身是公共資訊，但任何想要使用

證書來證明身份的人都必須可以使用相應的私鑰。但還必須對不能使用這種身份的任何人保密。

證書可以標識使用者或電腦。這取決於實施情況。大多數早期系統可能使用證書來識別電腦。如果證書標識了使用者，則與該證書對應的私鑰必須儲存為同一電腦上的其他使用者無法使用該私鑰。這通常意味著金鑰保持加密狀態，或者金鑰儲存在智慧卡中。加密金鑰案例在早期實現中可能更常見。在任一情況下，使用者通常必須在啟用金鑰時輸入密碼短語。

注意：ISAKMP/Oakley使用UDP埠500進行協商。AH在Protocol欄位中包含51，而ESP在Protocol欄位中包含50。確保沒有過濾這些內容。

有關此技術報告中使用的術語的詳細資訊，請參閱定義部分。

適用於IPSec和ISAKMP的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。

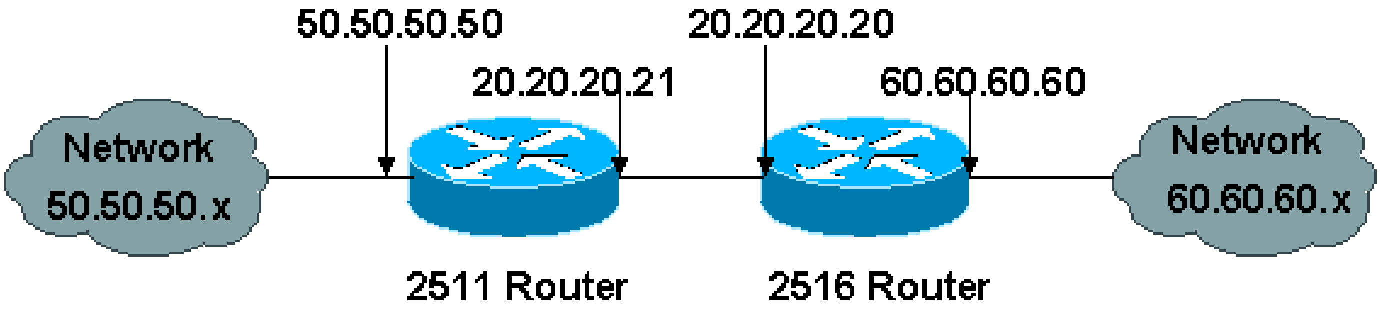
示例1:ISAKMP預先共用金鑰

通過預共用金鑰進行身份驗證是一種非公鑰替代方案。使用此方法，每個對等體共用一個金鑰，該金鑰已在帶外交換並配置到路由器中。每一端都能夠證明知道此密碼（不明確提及），從而對交換進行身份驗證。此方法適用於小型安裝，但確實存在擴充問題。下面使用預共用金鑰「sharedkey」。如果主機共用基於地址的預共用金鑰，則必須使用其地址標識，這是Cisco IOS軟體的預設標識，因此不會在配置中顯示：

```
crypto isakmp identity address
```

注意：在某些情況下，ISAKMP無法為IPSec建立策略和金鑰。如果路由器中沒有定義證書，且ISAKMP策略中只有基於公鑰的身份驗證方法，或者如果對等體沒有證書且沒有預共用金鑰（直接由地址共用或由已使用該地址配置的主機名共用），則ISAKMP無法與對等體協商，並且IPSec不起作用。

下圖顯示了此配置的網路圖。



以下是兩台路由器（Cisco 2511和Cisco 2516）的配置，它們根據預共用金鑰背靠背執行IPSec和ISAKMP身份驗證。註釋行以感歎號表示為第一個字元，如果輸入到路由器中，則會忽略註釋行。在下面的配置中，註釋位於某些配置行之前，以便對其進行描述。

Cisco 2511配置

```
cl-2513-2A#write terminal
Building configuration...

Current configuration:
!
version 11.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cl-2513-2A
!
!--- Override the default policy and use !--- preshared
keys for authentication. crypto isakmp policy 1
authentication pre-share group 2 ! !--- Define our
secret shared key so !--- you do not have to use RSA
keys. crypto isakmp key sharedkey address 20.20.20.20 !
!--- These are the authentication and encryption !---
settings defined for "auth2", !--- which is later
applied to the crypto map. crypto ipsec transform-set
auth2 esp-des esp-sha-hmac ! !--- The crypto map where
you define your peer, !--- transform auth2, and your
access list. crypto map test 10 ipsec-isakmp set peer
20.20.20.20 set transform-set auth2 match address 133 !
interface Ethernet0 ip address 50.50.50.50 255.255.255.0
! interface Serial0 ip address 20.20.20.21 255.255.255.0
no ip route-cache no ip mroute-cache !--- Nothing
happens unless you apply !--- the crypto map to an
interface. crypto map test ! ip route 0.0.0.0 0.0.0.0
20.20.20.20 ! !--- This is the access list referenced !-
-- in the crypto map; never use "any". !--- You are
encrypting traffic between !--- the remote Ethernet
LANs. access-list 133 permit ip 50.50.50.0 0.0.0.255
60.60.60.0 0.0.0.255 ! line con 0 line aux 0 line vty 0
4 login ! end
```

Cisco 2516配置

```
cl-2513-2B#show run
Building configuration...

Current configuration:
!
version 11.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cl-2513-2B
!
ip subnet-zero
!
!--- Override the default policy and use !--- preshared
keys for authentication. crypto isakmp policy 1
authentication pre-share group 2 !--- Define the secret
shared key so you !--- do not have to use RSA keys.
crypto isakmp key sharedkey address 20.20.20.21 !---
These are the authentication and encryption !---
settings defined for "auth2," !--- which is later
applied to the crypto map. crypto ipsec transform-set
auth2 esp-des esp-sha-hmac !--- The crypto map where you
define the peer, !--- transform auth2, and the access
```

```
list. crypto map test 10 ipsec-isakmp set peer
20.20.20.21 set transform-set auth2 match address 144 !
interface Ethernet0 ip address 60.60.60.60 255.255.255.0
no ip directed-broadcast ! !--- Nothing happens unless
you apply !--- the crypto map to an interface. interface
Serial0 ip address 20.20.20.20 255.255.255.0 no ip
directed-broadcast no ip route-cache no ip mroute-cache
clockrate 800000 crypto map test ! ip classless ip route
0.0.0.0 0.0.0.0 20.20.20.21 ! !--- This is the access
list referenced !--- in the crypto map; never use "any".
!--- You are encrypting traffic between !--- the remote
Ethernet LANs. access-list 144 permit ip 60.60.60.0
0.0.0.255 50.50.50.0 0.0.0.255 ! line con 0 transport
input none line aux 0 line vty 0 4 login ! end
```

以下是debug命令輸出。

```
--------------- Preshare with RSA key defined
(need to remove RSA keys) -----

*Mar  1 00:14:48.579: ISAKMP (10): incorrect policy settings.
 Unable to initiate.
*Mar  1 00:14:48.587: ISAKMP (11): incorrect policy settings.
 Unable to initiate......

--------------- Preshare, wrong hostname ---------------

ISAKMP: no pre-shared key based on hostname wan-2511.cisco.com!
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Aggressive mode
 failed with peer at
20.20.20.21
--------------- Preshare, incompatable policy --------------
wan2511#
*Mar  1 00:33:34.839: ISAKMP (17): processing SA payload. message ID = 0
*Mar  1 00:33:34.843: ISAKMP (17): Checking ISAKMP transform 1
 against priority 1 policy
*Mar  1 00:33:34.843: ISAKMP:      encryption DES-CBC
*Mar  1 00:33:34.843: ISAKMP:      hash SHA
*Mar  1 00:33:34.847: ISAKMP:      default group 2
*Mar  1 00:33:34.847: ISAKMP:      auth pre-share
*Mar  1 00:33:34.847: ISAKMP:      life type in seconds
*Mar  1 00:33:34.851: ISAKMP:      life duration (basic) of 240
*Mar  1 00:33:34.851: ISAKMP (17): atts are acceptable.
 Next payload is 0
*Mar  1 00:33:43.735: ISAKMP (17): processing KE payload.
 message ID = 0
*Mar  1 00:33:54.307: ISAKMP (17): processing NONCE payload.
 message ID = 0
*Mar  1 00:33:54.311: ISAKMP (17): processing ID payload.
 message ID = 0
*Mar  1 00:33:54.331: ISAKMP (17): SKEYID state generated
*Mar  1 00:34:04.867: ISAKMP (17): processing HASH payload.
 message ID = 0
*Mar  1 00:34:04.879: ISAKMP (17): SA has been authenticated
*Mar  1 00:34:06.151: ISAKMP (17): processing SA payload.
 message ID = -1357683133
*Mar  1 00:34:06.155: ISAKMP (17): Checking IPSec proposal 1
*Mar  1 00:34:06.155: ISAKMP: transform 1, AH_MD5_HMAC
*Mar  1 00:34:06.159: ISAKMP:   attributes in transform:
*Mar  1 00:34:06.159: ISAKMP:      encaps is 1
*Mar  1 00:34:06.159: ISAKMP:      SA life type in seconds
*Mar  1 00:34:06.163: ISAKMP:      SA life duration (basic) of 3600
```

```
*Mar  1 00:34:06.163: ISAKMP:      SA life type in kilobytes
*Mar  1 00:34:06.163: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:34:06.167: ISAKMP (17): atts not acceptable.
 Next payload is 0
*Mar  1 00:34:06.171: ISAKMP (17): Checking IPSec proposal 1
*Mar  1 00:34:06.171: ISAKMP: transform 1, ESP_DES
*Mar  1 00:34:06.171: ISAKMP:   attributes in transform:
*Mar  1 00:34:06.175: ISAKMP:      encaps is 1
*Mar  1 00:34:06.175: ISAKMP:      SA life type in seconds
*Mar  1 00:34:06.175: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:34:06.179: ISAKMP:      SA life type in kilobytes
*Mar  1 00:34:06.179: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:34:06.183: ISAKMP:      HMAC algorithm is SHA
*Mar  1 00:34:06.183: ISAKMP (17): atts are acceptable.
*Mar  1 00:34:06.187: ISAKMP (17): SA not acceptable!
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Quick mode failed
with peer at 20.20.20.20
wan2511#

----------------- preshare, debug isakmp -------------------

wan2511#
*Mar  1 00:06:54.179: ISAKMP (1): processing SA payload.
 message ID = 0
*Mar  1 00:06:54.179: ISAKMP (1): Checking ISAKMP transform 1
 against priority 1 policy
*Mar  1 00:06:54.183: ISAKMP:      encryption DES-CBC
*Mar  1 00:06:54.183: ISAKMP:      hash SHA
*Mar  1 00:06:54.183: ISAKMP:      default group 2
*Mar  1 00:06:54.187: ISAKMP:      auth pre-share
*Mar  1 00:06:54.187: ISAKMP:      life type in seconds
*Mar  1 00:06:54.187: ISAKMP:      life duration (basic) of 240
*Mar  1 00:06:54.191: ISAKMP (1): atts are acceptable.
 Next payload is 0
*Mar  1 00:07:02.955: ISAKMP (1): processing KE payload.
 message ID = 0
*Mar  1 00:07:13.411: ISAKMP (1): processing NONCE payload.
 message ID = 0
*Mar  1 00:07:13.415: ISAKMP (1): processing ID payload.
 message ID = 0
*Mar  1 00:07:13.435: ISAKMP (1): SKEYID state generated
*Mar  1 00:07:23.903: ISAKMP (1): processing HASH payload.
 message ID = 0
*Mar  1 00:07:23.915: ISAKMP (1): SA has been authenticated
*Mar  1 00:07:25.187: ISAKMP (1): processing SA payload.
 message ID = 1435594195
*Mar  1 00:07:25.187: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:07:25.191: ISAKMP: transform 1, AH_SHA_HMAC
*Mar  1 00:07:25.191: ISAKMP:   attributes in transform:
*Mar  1 00:07:25.191: ISAKMP:      encaps is 1
*Mar  1 00:07:25.195: ISAKMP:      SA life type in seconds
*Mar  1 00:07:25.195: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:07:25.195: ISAKMP:      SA life type in kilobytes
*Mar  1 00:07:25.199: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:07:25.203: ISAKMP (1): atts are acceptable.
*Mar  1 00:07:25.203: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:07:25.207: ISAKMP: transform 1, ESP_DES
*Mar  1 00:07:25.207: ISAKMP:   attributes in transform:
*Mar  1 00:07:25.207: ISAKMP:      encaps is 1
*Mar  1 00:07:25.211: ISAKMP:      SA life type in seconds
*Mar  1 00:07:25.211: ISAKMP:      SA life duration (basic) of 3600
```

```
*Mar  1 00:07:25.211: ISAKMP:      SA life type in kilobytes
*Mar  1 00:07:25.215: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:07:25.215: ISAKMP:      HMAC algorithm is SHA
*Mar  1 00:07:25.219: ISAKMP (1): atts are acceptable.
*Mar  1 00:07:25.223: ISAKMP (1): processing NONCE payload.
 message ID = 1435594195
*Mar  1 00:07:25.227: ISAKMP (1): processing ID payload.
 message ID = 1435594195
*Mar  1 00:07:25.227: ISAKMP (1): processing ID payload.
 message ID = 1435594195
*Mar  1 00:07:25.639: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:07:25.643:         inbound SA from 20.20.20.20
     to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:07:25.647:         has spi 85067251 and
 conn_id 3 and flags 4
*Mar  1 00:07:25.647:         lifetime of 3600 seconds
*Mar  1 00:07:25.647:         lifetime of 4608000 kilobytes
*Mar  1 00:07:25.651:         outbound SA from 20.20.20.21
     to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:07:25.655:         has spi 57872298 and
 conn_id 4 and flags 4
*Mar  1 00:07:25.655:         lifetime of 3600 seconds
*Mar  1 00:07:25.655:         lifetime of 4608000 kilobytes
*Mar  1 00:07:25.659: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:07:25.659:         inbound SA from 20.20.20.20
   to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:07:25.663:         has spi 538316566 and
 conn_id 5 and flags 4
*Mar  1 00:07:25.663:         lifetime of 3600 seconds
*Mar  1 00:07:25.667:         lifetime of 4608000 kilobytes
*Mar  1 00:07:25.667:         outbound SA from 20.20.20.21
 to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:07:25.671:         has spi 356000275 and
 conn_id 6 and flags 4
*Mar  1 00:07:25.671:         lifetime of 3600 seconds
*Mar  1 00:07:25.675:         lifetime of 4608000 kilobytes
wan2511#

----------------- preshare debug ipsec -------------------
wan2511#
*Mar  1 00:05:26.947: IPSEC(validate_proposal_request):
proposal part #1,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:05:26.955: IPSEC(validate_proposal_request):
proposal part #2,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:05:26.967: IPSEC(key_engine): got a queue event...
*Mar  1 00:05:26.971: IPSEC(spi_response): getting
 spi 203563166 for SA
```

```
        from 20.20.20.20     to 20.20.20.21     for prot 2
*Mar  1 00:05:26.975: IPSEC(spi_response): getting
 spi 194838793 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 3
*Mar  1 00:05:27.379: IPSEC(key_engine): got a queue event...
*Mar  1 00:05:27.379: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xC22209E(203563166), conn_id= 3, keysize= 0, flags= 0x4
*Mar  1 00:05:27.387: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x15E010D(22937869), conn_id= 4, keysize= 0, flags= 0x4
*Mar  1 00:05:27.395: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xB9D0109(194838793), conn_id= 5, keysize= 0, flags= 0x4
*Mar  1 00:05:27.403: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xDED0AB4(233638580), conn_id= 6, keysize= 0, flags= 0x4
*Mar  1 00:05:27.415: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 51,
    sa_spi= 0xC22209E(203563166),
    sa_trans= ah-sha-hmac , sa_conn_id= 3
*Mar  1 00:05:27.419: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 51,
    sa_spi= 0x15E010D(22937869),
    sa_trans= ah-sha-hmac , sa_conn_id= 4
*Mar  1 00:05:27.423: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 50,
    sa_spi= 0xB9D0109(194838793),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
*Mar  1 00:05:27.427: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 50,
    sa_spi= 0xDED0AB4(233638580),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
wan2511#

--------------- Preshare, good connection ------
wan2511#
*Mar  1 00:09:45.095: ISAKMP (1): processing SA payload.
 message ID = 0
*Mar  1 00:09:45.099: ISAKMP (1): Checking ISAKMP transform
 1 against priority 1 policy
*Mar  1 00:09:45.099: ISAKMP:      encryption DES-CBC
*Mar  1 00:09:45.103: ISAKMP:      hash SHA
*Mar  1 00:09:45.103: ISAKMP:      default group 2
*Mar  1 00:09:45.103: ISAKMP:      auth pre-share
*Mar  1 00:09:45.107: ISAKMP:      life type in seconds
*Mar  1 00:09:45.107: ISAKMP:      life duration (basic) of 240
*Mar  1 00:09:45.107: ISAKMP (1): atts are acceptable.
```

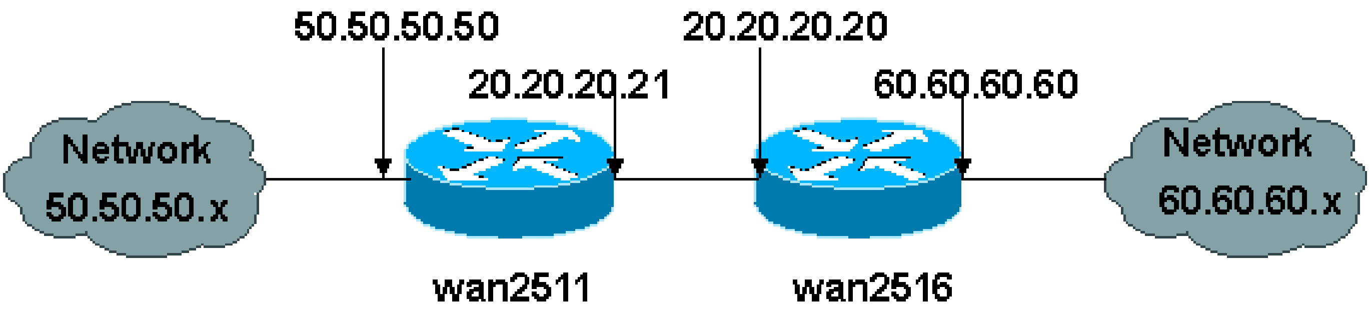
```
Next payload is 0
*Mar  1 00:09:53.867: ISAKMP (1): processing KE payload.
 message ID = 0
*Mar  1 00:10:04.323: ISAKMP (1): processing NONCE payload.
 message ID = 0
*Mar  1 00:10:04.327: ISAKMP (1): processing ID payload.
 message ID = 0
*Mar  1 00:10:04.347: ISAKMP (1): SKEYID state generated
*Mar  1 00:10:15.103: ISAKMP (1): processing HASH payload.
 message ID = 0
*Mar  1 00:10:15.115: ISAKMP (1): SA has been authenticated
*Mar  1 00:10:16.391: ISAKMP (1): processing SA payload.
 message ID = 800032287
*Mar  1 00:10:16.391: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:10:16.395: ISAKMP: transform 1, AH_SHA_HMAC
*Mar  1 00:10:16.395: ISAKMP:   attributes in transform:
*Mar  1 00:10:16.395: ISAKMP:      encaps is 1
*Mar  1 00:10:16.399: ISAKMP:      SA life type in seconds
*Mar  1 00:10:16.399: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:10:16.399: ISAKMP:      SA life type in kilobytes
*Mar  1 00:10:16.403: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:10:16.407: ISAKMP (1): atts are acceptable.
*Mar  1 00:10:16.407: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:10:16.411: ISAKMP: transform 1, ESP_DES
*Mar  1 00:10:16.411: ISAKMP:   attributes in transform:
*Mar  1 00:10:16.411: ISAKMP:      encaps is 1
*Mar  1 00:10:16.415: ISAKMP:      SA life type in seconds
*Mar  1 00:10:16.415: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:10:16.415: ISAKMP:      SA life type in kilobytes
*Mar  1 00:10:16.419: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:10:16.419: ISAKMP:      HMAC algorithm is SHA
*Mar  1 00:10:16.423: ISAKMP (1): atts are acceptable.
*Mar  1 00:10:16.427: IPSEC(validate_proposal_request):
 proposal part #1,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:10:16.435: IPSEC(validate_proposal_request):
 proposal part #2,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:10:16.443: ISAKMP (1): processing NONCE payload.
 message ID = 800032287
*Mar  1 00:10:16.443: ISAKMP (1): processing ID payload.
 message ID = 800032287
*Mar  1 00:10:16.447: ISAKMP (1): processing ID payload.
 message ID = 800032287
*Mar  1 00:10:16.451: IPSEC(key_engine): got a queue event...
*Mar  1 00:10:16.455: IPSEC(spi_response): getting
spi 16457800 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 2
*Mar  1 00:10:16.459: IPSEC(spi_response): getting
spi 305534655 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 3
*Mar  1 00:10:17.095: ISAKMP (1): Creating IPSec SAs
```

```
*Mar  1 00:10:17.095:         inbound SA from 20.20.20.20
     to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:10:17.099:         has spi 16457800 and conn_id 3
 and flags 4
*Mar  1 00:10:17.103:         lifetime of 3600 seconds
*Mar  1 00:10:17.103:         lifetime of 4608000 kilobytes
*Mar  1 00:10:17.103:         outbound SA from 20.20.20.21
     to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:10:17.107:         has spi 507120385 and conn_id 4
 and flags 4
*Mar  1 00:10:17.111:         lifetime of 3600 seconds
*Mar  1 00:10:17.111:         lifetime of 4608000 kilobytes
*Mar  1 00:10:17.115: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:10:17.115:         inbound SA from 20.20.20.20
to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:10:17.119:         has spi 305534655 and
conn_id 5 and flags 4
*Mar  1 00:10:17.119:         lifetime of 3600 seconds
*Mar  1 00:10:17.123:         lifetime of 4608000 kilobytes
*Mar  1 00:10:17.123:         outbound SA from 20.20.20.21
     to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:10:17.127:         has spi 554175376 and
conn_id 6 and flags 4
*Mar  1 00:10:17.127:         lifetime of 3600 seconds
*Mar  1 00:10:17.131:         lifetime of 4608000 kilobytes
*Mar  1 00:10:17.139: IPSEC(key_engine): got a queue event...
*Mar  1 00:10:17.143: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xFB2048(16457800), conn_id= 3, keysize= 0,
 flags= 0x4
*Mar  1 00:10:17.151: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x1E3A0B01(507120385), conn_id= 4, keysize= 0,
 flags= 0x4
*Mar  1 00:10:17.159: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x123616BF(305534655), conn_id= 5, keysize= 0,
 flags= 0x4
*Mar  1 00:10:17.167: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x21080B90(554175376), conn_id= 6, keysize= 0,
 flags= 0x4
*Mar  1 00:10:17.175: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 51,
    sa_spi= 0xFB2048(16457800),
    sa_trans= ah-sha-hmac , sa_conn_id= 3
*Mar  1 00:10:17.179: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 51,
    sa_spi= 0x1E3A0B01(507120385),
    sa_trans= ah-sha-hmac , sa_conn_id= 4
*Mar  1 00:10:17.183: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 50,
    sa_spi= 0x123616BF(305534655),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
*Mar  1 00:10:17.187: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 50,
    sa_spi= 0x21080B90(554175376),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
*Mar  1 00:10:36.583: ISADB: reaper checking SA, conn_id = 1
wan2511#
```

示例2:ISAKMP:RSA加密身份驗證

在這種情況下，不會建立共用金鑰。每台路由器生成自己的RSA金鑰。然後每台路由器都需要配置對等裝置的RSA公鑰。這是一個手動過程，具有明顯的擴展限制。換句話說，路由器需要為其希望與其建立安全關聯的每個對等體提供公共RSA金鑰。

以下文檔表示此示例配置的網路圖。



在本示例中，每台路由器生成一個RSA金鑰對（您永遠不會看到您生成的RSA私鑰），並配置遠端對等體的公用RSA金鑰。

```
wan2511(config)#crypto key generate rsa
The name for the keys will be: wan2511.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
Generating RSA keys ...
[OK]

wan2511(config)#^Z
wan2511#
wan2511#show crypto key mypubkey rsa
% Key pair was generated at: 00:09:04 UTC Mar 1 1993
Key name: wan2511.cisco.com
Usage:    General Purpose Key
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8
 6E1C0423 92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B
 3A2BD92F 98039DAC 08741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001
```

```
wan2511#

wan2511(config)#crypto key pubkey-chain rsa
wan2511(config-pubkey-chain)#named-key wan2516.cisco.com
wan2511(config-pubkey-key)#key-string
Enter a public key as a hexidecimal number ....

wan2511(config-pubkey)#$86F70D 01010105 00034B00 30480241 00DC3DDC 59885F14
wan2511(config-pubkey)#$D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699
wan2511(config-pubkey)#$220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001
wan2511(config-pubkey)#quit
wan2511(config-pubkey-key)#^Z
wan2511#
wan2511#show crypto key pubkey-chain rsa
Key name: wan2516.cisco.com
Key usage: general purpose
Key source: manually entered
Key data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DC3DDC 59885F14
 1AB30DCB 794AB5C7 82D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699
 3BC9D17E C47581DC 50220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001


wan2511#
wan2511#write terminal
Building configuration...

Current configuration:
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname wan2511
!
enable password ww
!
no ip domain-lookup
ip host wan2516.cisco.com 20.20.20.20
ip domain-name cisco.com
!
crypto isakmp policy 1
 authentication rsa-encr
 group 2
 lifetime 240
crypto isakmp identity hostname
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map test 10 ipsec-isakmp
 set peer 20.20.20.20
 set transform-set auth2
 match address 133
!
crypto key pubkey-chain rsa
 named-key wan2516.cisco.com
  key-string
   305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DC3DDC 59885F14
   1AB30DCB 794AB5C7 82D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699
   3BC9D17E C47581DC 50220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001
  quit
!
interface Ethernet0
 ip address 50.50.50.50 255.255.255.0
```

```
!
interface Serial0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 crypto map test
!
interface Serial1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.11.19.254
ip route 60.0.0.0 255.0.0.0 20.20.20.20
access-list 133 permit ip 50.50.50.0 0.0.0.255 60.60.60.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
 password ww
 login
line 1 6
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware
line 7 16
 autoselect ppp
 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



wan2511#
-----------------

wan2516(config)#crypto key generate rsa
The name for the keys will be: wan2516.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
Generating RSA keys ...
[OK]

wan2516#show crypto key mypubkey rsa
% Key pair was generated at: 00:06:35 UTC Mar 1 1993
Key name: wan2516.cisco.com
Usage:    General Purpose Key
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DC3DDC 59885F14
 1AB30DCB 794AB5C7 82D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699
 3BC9D17E C47581DC 50220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001
wan2516#

-------
wan2516(config)#crypto key exchange ?
  dss  Exchange DSS keys
-------

wan2516(config)#crypto key pubkey-chain rsa
wan2516(config-pubkey-chain)#named-key wan2511.cisco.com
wan2516(config-pubkey-key)#key-string
Enter a public key as a hexidecimal number ....

wan2516(config-pubkey)#$86F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8
wan2516(config-pubkey)#$C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B
wan2516(config-pubkey)#$741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001
wan2516(config-pubkey)#quit
wan2516(config-pubkey-key)#^Z

wan2516#show crypto key pubkey rsa
Key name: wan2511.cisco.com
Key usage: general purpose
Key source: manually entered
Key data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8
 6E1C0423 92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B
 3A2BD92F 98039DAC 08741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001



wan2516#
------------------------
wan2516#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service pad
service timestamps debug datetime msec
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname wan2516
!
enable password ww
!
no ip domain-lookup
ip host wan2511.cisco.com 20.20.20.21
ip domain-name cisco.com
!
crypto isakmp policy 1
 authentication rsa-encr
 group 2
 lifetime 240
crypto isakmp identity hostname
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map test 10 ipsec-isakmp
 set peer 20.20.20.21
 set transform-set auth2
 match address 144
```

```
!
crypto key pubkey-chain rsa
 named-key wan2511.cisco.com
  key-string
   305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8
   6E1C0423 92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B
   3A2BD92F 98039DAC 08741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001
  quit
!
hub ether 0 1
 link-test
 auto-polarity
!
interface Loopback0
 ip address 70.70.70.1 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet0
 ip address 60.60.60.60 255.255.255.0
!
interface Serial0
 ip address 20.20.20.20 255.255.255.0
 encapsulation ppp
 clockrate 2000000
 crypto map test
!
interface Serial1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface BRI0
 no ip address
 no ip route-cache
 no ip mroute-cache
 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 60.60.60.0 0.0.0.255 50.50.50.0 0.0.0.255
!
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

wan2516#

--------------- RSA-enc missing RSA Keys ---------
```

```
*Mar  1 00:02:51.147: ISAKMP: No cert, and no keys (public or pre-shared)
        with remote peer 20.20.20.21
*Mar  1 00:02:51.151: ISAKMP: No cert, and no keys (public or pre-shared)
        with remote peer 20.20.20.21

--------------- RSA-enc good connection -----------------
wan2511#
*Mar  1 00:21:46.375: ISAKMP (1): processing SA payload.
message ID = 0
*Mar  1 00:21:46.379: ISAKMP (1): Checking ISAKMP
transform 1 against
      priority 1 policy
*Mar  1 00:21:46.379: ISAKMP:      encryption DES-CBC
*Mar  1 00:21:46.379: ISAKMP:      hash SHA
*Mar  1 00:21:46.383: ISAKMP:      default group 2
*Mar  1 00:21:46.383: ISAKMP:      auth RSA encr
*Mar  1 00:21:46.383: ISAKMP:      life type in seconds
*Mar  1 00:21:46.387: ISAKMP:      life duration (basic)
of 240
*Mar  1 00:21:46.387: ISAKMP (1): atts are acceptable.
Next payload is 0
*Mar  1 00:21:46.391: Crypto engine 0: generate alg param

*Mar  1 00:21:55.159: CRYPTO_ENGINE: Dh phase 1 status: 0
*Mar  1 00:21:55.163: CRYPTO: DH gen phase 1 status for
conn_id 1 slot 0:OK
*Mar  1 00:21:55.167: ISAKMP (1): Unable to get router
cert to find DN!
*Mar  1 00:21:55.171: ISAKMP (1): SA is doing RSA
encryption authentication
*Mar  1 00:22:04.351: ISAKMP (1): processing KE payload.
message ID = 0
*Mar  1 00:22:04.351: Crypto engine 0: generate alg param

*Mar  1 00:22:14.767: CRYPTO: DH gen phase 2 status for
conn_id 1 slot 0:OK
*Mar  1 00:22:14.771: ISAKMP (1): processing ID payload.
message ID = 0
*Mar  1 00:22:14.775: Crypto engine 0: RSA decrypt
with private key
*Mar  1 00:22:15.967: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:16.167: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:16.367: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:16.579: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:16.787: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:16.987: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:17.215: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:17.431: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:17.539: CRYPTO: RSA private decrypt
finished with status=OK
*Mar  1 00:22:17.543: ISAKMP (1): processing NONCE
payload. message ID = 0
*Mar  1 00:22:17.543: Crypto engine 0: RSA decrypt
with private key
*Mar  1 00:22:18.735: CRYPTO_ENGINE: key process
suspended and continued
```

```
*Mar  1 00:22:18.947: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:19.155: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:19.359: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:19.567: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:19.767: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:19.975: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:20.223: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:20.335: CRYPTO: RSA private decrypt
finished with status=OK
*Mar  1 00:22:20.347: Crypto engine 0: create ISAKMP
SKEYID for conn id 1
*Mar  1 00:22:20.363: ISAKMP (1): SKEYID state generated
*Mar  1 00:22:20.367: Crypto engine 0: RSA encrypt
with public key
*Mar  1 00:22:20.567: CRYPTO: RSA public encrypt
finished with status=OK
*Mar  1 00:22:20.571: Crypto engine 0: RSA encrypt
with public key
*Mar  1 00:22:20.767: CRYPTO: RSA public encrypt
finished with status=OK
*Mar  1 00:22:20.775: ISAKMP (1): processing KE
payload. message ID = 0
*Mar  1 00:22:20.775: ISAKMP (1): processing ID
payload. message ID = 0
*Mar  1 00:22:20.779: Crypto engine 0: RSA decrypt
with private key
*Mar  1 00:22:21.959: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:22.187: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:22.399: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:22.599: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:22.811: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:23.019: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:23.223: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:23.471: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:23.583: CRYPTO: RSA private decrypt
finished with status=OK
*Mar  1 00:22:23.583: ISAKMP (1): processing NONCE
payload. message ID = 0
%CRYPTO-6-IKMP_AUTH_FAIL: Authentication method 4
failed with host 20.20.20.20
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main
mode failed with peer
  at 20.20.20.20
*Mar  1 00:22:36.955: ISAKMP (1): processing HASH
payload. message ID = 0
*Mar  1 00:22:36.959: generate hmac context for conn id 1
*Mar  1 00:22:36.971: ISAKMP (1): SA has been authenticated
*Mar  1 00:22:36.975: generate hmac context for conn id 1
*Mar  1 00:22:37.311: generate hmac context for conn id 1
```

```
*Mar  1 00:22:37.319: ISAKMP (1): processing SA payload.
message ID = -114148384
*Mar  1 00:22:37.319: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:22:37.323: ISAKMP: transform 1, AH_SHA_HMAC
*Mar  1 00:22:37.323: ISAKMP: attributes in transform:
*Mar  1 00:22:37.327: ISAKMP: encaps is 1
*Mar  1 00:22:37.327: ISAKMP: SA life type in seconds
*Mar  1 00:22:37.327: ISAKMP: SA life duration (basic) of 3600
*Mar  1 00:22:37.331: ISAKMP: SA life type in kilobytes
*Mar  1 00:22:37.331: ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:22:37.335: ISAKMP (1): atts are acceptable.
*Mar  1 00:22:37.335: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:22:37.339: ISAKMP: transform 1, ESP_DES
*Mar  1 00:22:37.339: ISAKMP: attributes in transform:
*Mar  1 00:22:37.339: ISAKMP: encaps is 1
*Mar  1 00:22:37.343: ISAKMP: SA life type in seconds
*Mar  1 00:22:37.343: ISAKMP: SA life duration (basic) of 3600
*Mar  1 00:22:37.347: ISAKMP: SA life type in kilobytes
*Mar  1 00:22:37.347: ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:22:37.351: ISAKMP: HMAC algorithm is SHA
*Mar  1 00:22:37.351: ISAKMP (1): atts are acceptable.
*Mar  1 00:22:37.355: IPSEC(validate_proposal_request):
proposal part #1,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:22:37.363: IPSEC(validate_proposal_request):
proposal part #2,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:22:37.371: ISAKMP (1): processing NONCE payload.
      message ID = -114148384
*Mar  1 00:22:37.375: ISAKMP (1): processing ID payload.
message ID = -114148384
*Mar  1 00:22:37.375: ISAKMP (1): processing ID payload.
 message ID = -114148384
*Mar  1 00:22:37.379: IPSEC(key_engine): got a queue event...
*Mar  1 00:22:37.383: IPSEC(spi_response): getting spi
531040311 for SA
        from 20.20.20.20     to 20.20.20.21 for prot 2
*Mar  1 00:22:37.387: IPSEC(spi_response): getting spi
220210147 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 3
*Mar  1 00:22:37.639: generate hmac context for conn id 1
*Mar  1 00:22:37.931: generate hmac context for conn id 1
*Mar  1 00:22:37.975: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:22:37.975: inbound SA from 20.20.20.20
   to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:22:37.979:  has spi 531040311 and conn_id 2 and flags 4
*Mar  1 00:22:37.979:   lifetime of 3600 seconds
*Mar  1 00:22:37.983:    lifetime of 4608000 kilobytes
*Mar  1 00:22:37.983:  outbound SA from 20.20.20.21
 to 20.20.20.20
        (proxy 50.50.50.0 to 60.60.60.0     )
```

```
*Mar  1 00:22:37.987: has spi 125043658 and
conn_id 3 and flags 4
*Mar  1 00:22:37.987: lifetime of 3600 seconds
*Mar  1 00:22:37.991: lifetime of 4608000 kilobytes
*Mar  1 00:22:37.991: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:22:37.991: inbound SA from 20.20.20.20 to 20.20.20.21
        (proxy 60.60.60.0 to 50.50.50.0     )
*Mar  1 00:22:37.995: has spi 220210147 and conn_id 4 and flags 4
*Mar  1 00:22:37.999: lifetime of 3600 seconds
*Mar  1 00:22:37.999: lifetime of 4608000 kilobytes
*Mar  1 00:22:38.003: outbound SA from 20.20.20.21 to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:22:38.003: has spi 299247102 and
conn_id 5 and flags 4
*Mar  1 00:22:38.007: lifetime of 3600 seconds
*Mar  1 00:22:38.007: lifetime of 4608000 kilobytes
*Mar  1 00:22:38.011: IPSEC(key_engine): got a queue event...
*Mar  1 00:22:38.015: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x1FA70837(531040311), conn_id= 2, keysize= 0, flags= 0x4
*Mar  1 00:22:38.023: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x77403CA(125043658), conn_id= 3, keysize= 0, flags= 0x4
*Mar  1 00:22:38.031: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xD2023E3(220210147), conn_id= 4, keysize= 0, flags= 0x4
*Mar  1 00:22:38.039: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x11D625FE(299247102), conn_id= 5, keysize= 0, flags= 0x4
*Mar  1 00:22:38.047: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 51,
    sa_spi= 0x1FA70837(531040311),
    sa_trans= ah-sha-hmac , sa_conn_id= 2
*Mar  1 00:22:38.051: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 51,
    sa_spi= 0x77403CA(125043658),
    sa_trans= ah-sha-hmac , sa_conn_id= 3
*Mar  1 00:22:38.055: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 50,
    sa_spi= 0xD2023E3(220210147),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 4
*Mar  1 00:22:38.063: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 50,
    sa_spi= 0x11D625FE(299247102),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
wan2511#

----------- RSA-ENC ISAKMP debugs good connection ---
```

```
wan2511#
*Mar  1 00:27:23.279: ISAKMP (6): processing SA payload.
 message ID = 0
*Mar  1 00:27:23.279: ISAKMP (6): Checking ISAKMP
 transform 1 against
      priority 1 policy
*Mar  1 00:27:23.283: ISAKMP: encryption DES-CBC
*Mar  1 00:27:23.283: ISAKMP: hash SHA
*Mar  1 00:27:23.283: ISAKMP: default group 2
*Mar  1 00:27:23.287: ISAKMP: auth RSA encr
*Mar  1 00:27:23.287: ISAKMP: life type in seconds
*Mar  1 00:27:23.287: ISAKMP: life duration (basic) of 240
*Mar  1 00:27:23.291: ISAKMP (6): atts are acceptable.
Next payload is 0
*Mar  1 00:27:32.055: ISAKMP (6): Unable to get
router cert to find DN!
*Mar  1 00:27:32.055: ISAKMP (6): SA is doing RSA
encryption authentication
*Mar  1 00:27:41.183: ISAKMP (6): processing KE payload.
message ID = 0
*Mar  1 00:27:51.779: ISAKMP (6): processing ID payload.
 message ID = 0
*Mar  1 00:27:54.507: ISAKMP (6): processing NONCE payload.
 message ID = 0
*Mar  1 00:27:57.239: ISAKMP (6): SKEYID state generated
*Mar  1 00:27:57.627: ISAKMP (6): processing KE payload.
 message ID = 0
*Mar  1 00:27:57.631: ISAKMP (6): processing ID payload.
 message ID = 0
*Mar  1 00:28:00.371: ISAKMP (6): processing NONCE payload.

 message ID = 0
%CRYPTO-6-IKMP_AUTH_FAIL: Authentication method 4 failed
with host 20.20.20.20
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed
 with peer at 20.20.20.20
*Mar  1 00:28:13.587: ISAKMP (6): processing HASH payload.
 message ID = 0
*Mar  1 00:28:13.599: ISAKMP (6): SA has been authenticated
*Mar  1 00:28:13.939: ISAKMP (6): processing SA payload.
 message ID = -161552401
*Mar  1 00:28:13.943: ISAKMP (6): Checking IPSec proposal 1
*Mar  1 00:28:13.943: ISAKMP: transform 1, AH_SHA_HMAC
*Mar  1 00:28:13.943: ISAKMP:   attributes in transform:
*Mar  1 00:28:13.947: ISAKMP: encaps is 1
*Mar  1 00:28:13.947: ISAKMP: SA life type in seconds
*Mar  1 00:28:13.947: ISAKMP: SA life duration (basic) of 3600
*Mar  1 00:28:13.951: ISAKMP: SA life type in kilobytes
*Mar  1 00:28:13.951: ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:28:13.955: ISAKMP (6): atts are acceptable.
*Mar  1 00:28:13.959: ISAKMP (6): Checking IPSec proposal 1
*Mar  1 00:28:13.959: ISAKMP: transform 1, ESP_DES
*Mar  1 00:28:13.959: ISAKMP: attributes in transform:
*Mar  1 00:28:13.963: ISAKMP: encaps is 1
*Mar  1 00:28:13.963: ISAKMP: SA life type in seconds
*Mar  1 00:28:13.963: ISAKMP: SA life duration (basic) of 3600
*Mar  1 00:28:13.967: ISAKMP: SA life type in kilobytes
*Mar  1 00:28:13.967: ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:28:13.971: ISAKMP:      HMAC algorithm is SHA
*Mar  1 00:28:13.971: ISAKMP (6): atts are acceptable.
*Mar  1 00:28:13.975: ISAKMP (6): processing NONCE payload.
 message ID = -161552401
```

```
*Mar  1 00:28:13.979: ISAKMP (6): processing ID payload.
 message ID = -161552401
*Mar  1 00:28:13.979: ISAKMP (6): processing ID payload.
 message ID = -161552401
*Mar  1 00:28:14.391: ISAKMP (6): Creating IPSec SAs
*Mar  1 00:28:14.391: inbound SA from 20.20.20.20 to 20.20.20.21
        (proxy 60.60.60.0 to 50.50.50.0     )
*Mar  1 00:28:14.395: has spi 437593758 and conn_id 7 and flags 4
*Mar  1 00:28:14.399: lifetime of 3600 seconds
*Mar  1 00:28:14.399: lifetime of 4608000 kilobytes
*Mar  1 00:28:14.403: outbound SA from 20.20.20.21 to 20.20.20.20
        (proxy 50.50.50.0 to 60.60.60.0     )
*Mar  1 00:28:14.403: has spi 411835612 and conn_id 8 and flags 4
*Mar  1 00:28:14.407: lifetime of 3600 seconds
*Mar  1 00:28:14.407: lifetime of 4608000 kilobytes
*Mar  1 00:28:14.411: ISAKMP (6): Creating IPSec SAs
*Mar  1 00:28:14.411: inbound SA from 20.20.20.20 to 20.20.20.21
        (proxy 60.60.60.0 to 50.50.50.0     )
*Mar  1 00:28:14.415: has spi 216990519 and conn_id 9 and flags 4
*Mar  1 00:28:14.415: lifetime of 3600 seconds
*Mar  1 00:28:14.419: lifetime of 4608000 kilobytes
*Mar  1 00:28:14.419: outbound SA from 20.20.20.21 to 20.20.20.20
        (proxy 50.50.50.0 to 60.60.60.0     )
*Mar  1 00:28:14.423: has spi 108733569 and conn_id 10 and flags 4
*Mar  1 00:28:14.423: lifetime of 3600 seconds
*Mar  1 00:28:14.427: lifetime of 4608000 kilobytes
wan2511#

-------------------------- RSA-enc IPSEC debug -------
wan2511#
*Mar  1 00:30:32.155: ISAKMP (11): Unable to get
router cert to find DN!
wan2511#show debug
Cryptographic Subsystem:
  Crypto IPSEC debugging is on
wan2511#
wan2511#
wan2511#
wan2511#
%CRYPTO-6-IKMP_AUTH_FAIL: Authentication method
4 failed with host 20.20.20.20
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main
mode failed with peer at
20.20.20.20
*Mar  1 00:31:13.931: IPSEC(validate_proposal_request):
 proposal part #1,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:31:13.935: IPSEC(validate_proposal_request):
 proposal part #2,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:31:13.947: IPSEC(key_engine): got a queue event...
*Mar  1 00:31:13.951: IPSEC(spi_response): getting
spi 436869446 for SA
        from 20.20.20.20     to 20.20.20.21 for prot 2
```

```
*Mar  1 00:31:13.955: IPSEC(spi_response): getting
 spi 285609740 for SA
        from 20.20.20.20     to 20.20.20.21 for prot 3
*Mar  1 00:31:14.367: IPSEC(key_engine): got a queue event...
*Mar  1 00:31:14.367: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x1A0A1946(436869446), conn_id= 12, keysize= 0,
flags= 0x4
*Mar  1 00:31:14.375: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x2C40706(46401286), conn_id= 13, keysize= 0,
flags= 0x4
*Mar  1 00:31:14.383: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x11060F0C(285609740), conn_id= 14, keysize= 0,
flags= 0x4
*Mar  1 00:31:14.391: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x12881335(310907701), conn_id= 15, keysize= 0,
 flags= 0x4
*Mar  1 00:31:14.399: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 51,
    sa_spi= 0x1A0A1946(436869446),
    sa_trans= ah-sha-hmac , sa_conn_id= 12
*Mar  1 00:31:14.407: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 51,
    sa_spi= 0x2C40706(46401286),
    sa_trans= ah-sha-hmac , sa_conn_id= 13
*Mar  1 00:31:14.411: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 50,
    sa_spi= 0x11060F0C(285609740),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 14
*Mar  1 00:31:14.415: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 50,
    sa_spi= 0x12881335(310907701),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 15
wan2511#
```

示例3:ISAKMP:RSA-SIG身份驗證/CA

此示例使用RSA簽名，該簽名要求使用CA伺服器。每個對等點都從CA伺服器獲取證書（這通常是配置為頒發證書的工作站）。 當兩個對等體都具有有效的CA證書時，它們會自動相互交換RSA公鑰，作為ISAKMP協商的一部分。此案例只需每個對等點向CA註冊並獲得證書。對等體不再需要保留網路中所有對等體的公共RSA金鑰。

另請注意，由於您正在使用預設策略，因此未指定ISAKMP策略，如下所示：

```
lab-isdn1#show crypto isakmp policy
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

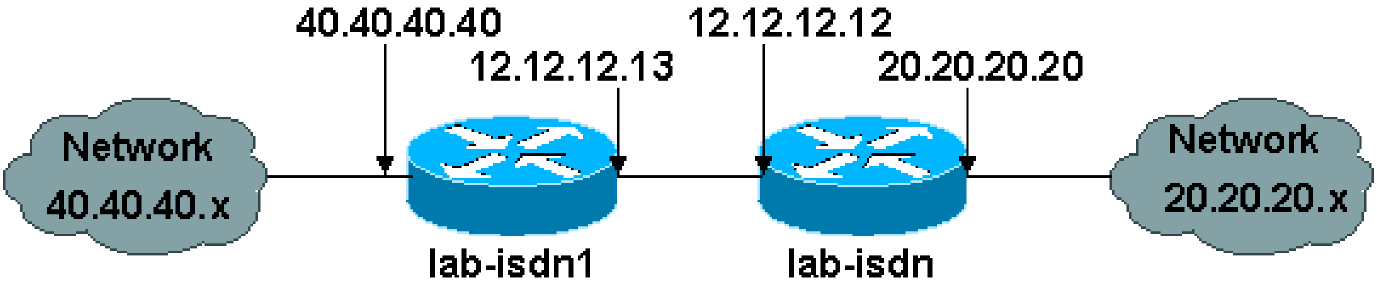
首先，定義CA伺服器的主機名，並生成RSA金鑰。

```
test1-isdn(config)#ip host cert-author 10.19.54.46
test1-isdn(config)#crypto key gen rsa usage
The name for the keys will be: test1-isdn.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  Signature Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
Generating RSA keys ...
[OK]
Choose the size of the key modulus in the range of 360 to 2048 for your
  Encryption Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
Generating RSA keys ...
[OK]
```

接下來，使用名為「test1-isdn-ultra」的標籤定義CA配置，並定義CA名稱URL。然後，與CA伺服器進行驗證並獲得憑證。最後，請繼續檢查，以確保已收到「可用」證書可供使用。

```
test1-isdn(config)#crypto ca identity test1-isdn-ultra
test1-isdn(ca-identity)#enrollment url http://cert-author
test1-isdn(ca-identity)#crl optional
test1-isdn(ca-identity)#exit

-----------------------------------
test1-isdn(config)#crypto ca authenticate test1-isdn-ultra
Certificate has the following attributes:
Fingerprint: 71CA5A98 78828EF8 4987BA95 57830E5F
% Do you accept this certificate? [yes/no]: yes
Apr  3 14:08:56.329: CRYPTO_PKI: http connection opened
Apr  3 14:08:56.595: CRYPTO__PKI: All enrollment requests completed.
Apr  3 14:08:56.599: CRYPTO_PKI: transaction GetCACert completed
Apr  3 14:08:56.599: CRYPTO_PKI: CA certificate received
test1-isdn(config)#

------------------------------------
test1-isdn(config)#crypto ca enroll test1-isdn-ultra
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will be: test1-isdn.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 04922418
% Include an IP address in the subject name? [yes/no]: yes
Interface: bri0
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

----------------- status: pending ---------------

test1-isdn#show crypto ca certificate
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F
  Key Usage: Not Set

Certificate
  Subject Name
    Name: test1-isdn.cisco.com
    IP Address: 10.18.117.189
    Serial Number: 04922418
  Status: Pending
  Key Usage: Signature
    Fingerprint:  B1566229 472B1DDB 01A072C0 8202A985 00000000

Certificate
  Subject Name
    Name: test1-isdn.cisco.com
    IP Address: 10.18.117.189
    Serial Number: 04922418
  Status: Pending
  Key Usage: Encryption
    Fingerprint:  1EA39C07 D1B26FC7 7AD08BF4 ACA3AABD 00000000


----------------- status: available ---------------
test1-isdn#show crypto ca certificate
Certificate
  Subject Name
    Name: test1-isdn.cisco.com
    Serial Number: 04922418
  Status: Available
  Certificate Serial Number: 1BAFCBCA71F0434B59D192FAFB37D376
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F
  Key Usage: Not Set

Certificate
  Subject Name
    Name: test1-isdn.cisco.com
    Serial Number: 04922418
  Status: Available
  Certificate Serial Number: 4B39EE2866814279CBA7534496DE1D99
  Key Usage: Signature

test1-isdn#
```

下圖顯示了此示例配置的網路圖。



以下示例配置取自兩台Cisco 1600路由器，它們之前已獲得CA證書（如上所示），並打算使用「rsa-sig」作為身份驗證策略執行ISAKMP。僅加密兩個遠端乙太網LAN之間的流量。

```
lab-isdn1#write terminal
Building configuration...

Current configuration:
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname lab-isdn1
!
enable secret 5 $1$VdPY$uA/BIVeEm9UAFEm.PPJFc.
!
username lab-isdn password 0 cisco
ip host ciscoca-ultra 171.69.54.46
ip host lab-isdn 12.12.12.12
ip domain-name cisco.com
ip name-server 171.68.10.70
ip name-server 171.68.122.99
isdn switch-type basic-ni1
!
crypto ipsec transform-set mypolicy ah-sha-hmac esp-des esp-sha-hmac
!
crypto map test 10 ipsec-isakmp
 set peer 12.12.12.12
 set transform-set mypolicy
 match address 144
!
crypto ca identity bubba
 enrollment url http://ciscoca-ultra
 crl optional
crypto ca certificate chain bubba
 certificate 3E1ED472BDA2CE0163FB6B0B004E5EEE
  308201BC 30820166 A0030201 0202103E
 1ED472BD A2CE0163 FB6B0B00 4E5EEE30
  0D06092A 864886F7 0D010104 05003042
  31163014 06035504 0A130D43 6973636F
  20537973 74656D73 3110300E 06035504
  0B130744 65767465 73743116 30140603
  55040313 0D434953 434F4341 2D554C54
  5241301E 170D3938 30343038 30303030
  30305A17 0D393930 34303832 33353935
  395A303B 31273025 06092A86 4886F70D
  01090216 18737461 6E6E6F75 732D6973
  646E312E 63697363 6F2E636F 6D311030
  0E060355 04051307 35363739 39383730
  5C300D06 092A8648 86F70D01 01010500
  034B0030 48024100 D2D125FF BBFC6E56
  93CB4385 5473C165 BC7CCAF6 45C35BED
  554BAA0B 119AFA6F 0853F574 5E0B8492
  2E39B5FA 84C4DD05 C19AA625 8184395C
  6CBC7FA4 614F6177 02030100 01A33F30
  3D300B06 03551D0F 04040302 05203023
  0603551D 11041C30 1A821873 74616E6E
  6F75732D 6973646E 312E6369 73636F2E
  636F6D30 09060355 1D130402 3000300D
  06092A86 4886F70D 01010405 00034100
  04AF83B8 FE95F5D9 9C07C105 F1E88F1A
  9320CE7D 0FA540CF 44C77829 FC85C94B
  8CB4CA32 85FF9655 8E47AC9A B9D6BF1A
  0C4846DE 5CB07C8E A32038EC 8AFD161A
  quit
 certificate ca 3051DF7169BEE31B821DFE4B3A338E5F
  30820182 3082012C A0030201 02021030
  51DF7169 BEE31B82 1DFE4B3A 338E5F30
  0D06092A 864886F7 0D010104 05003042
  31163014 06035504 0A130D43 6973636F
  20537973 74656D73 3110300E 06035504
  0B130744 65767465 73743116 30140603
  55040313 0D434953 434F4341 2D554C54
  5241301E 170D3937 31323032 30313036
  32385A17 0D393831 32303230 31303632
  385A3042 31163014 06035504 0A130D43
  6973636F 20537973 74656D73 3110300E
  06035504 0B130744 65767465 73743116
  30140603 55040313 0D434953 434F4341
  2D554C54 5241305C 300D0609 2A864886
  F70D0101 01050003 4B003048 024100C1
  B69D7BF6 34E4EE28 A84E0DC6 FCA4DEA8
  04D89E50 C5EBE862 39D51890 D0D4B732
  678BDBF2 80801430 E5E56E7C C126E2DD
  DBE9695A DF8E5BA7 E67BAE87 29375302
  03010001 300D0609 2A864886 F70D0101
  04050003 410035AA 82B5A406 32489413
  A7FF9A9A E349E5B4 74615E05 058BA3CE
  7C5F00B4 019552A5 E892D2A3 86763A1F
  2852297F C68EECE1 F41E9A7B 2F38D02A
  B1D2F817 3F7B
  quit
 certificate 503968D890F7D409475B7280162754D2
  308201BC 30820166 A0030201 02021050
  3968D890 F7D40947 5B728016 2754D230
  0D06092A 864886F7 0D010104 05003042
  31163014 06035504 0A130D43 6973636F
  20537973 74656D73 3110300E 06035504
  0B130744 65767465 73743116 30140603
  55040313 0D434953 434F4341 2D554C54
  5241301E 170D3938 30343038 30303030
  30305A17 0D393930 34303832 33353935
  395A303B 31273025 06092A86 4886F70D
  01090216 18737461 6E6E6F75 732D6973
  646E312E 63697363 6F2E636F 6D311030
  0E060355 04051307 35363739 39383730
  5C300D06 092A8648 86F70D01 01010500
  034B0030 48024100 BECE2D8C B32E6B09
  0ADE0D46 AF8D4A1F 37850034 35D0C729
  3BF91518 0C9E4CF8 1A6A43AE E4F04687
  B8E2859D 33D5CE04 2E5DDEA6 3DA54A31
  2AD4255A 756014CB 02030100 01A33F30
  3D300B06 03551D0F 04040302 07803023
  0603551D 11041C30 1A821873 74616E6E
  6F75732D 6973646E 312E6369 73636F2E
  636F6D30 09060355 1D130402 3000300D
  06092A86 4886F70D 01010405 00034100
  B3AF6E71 CBD9AEDD A4711B71 6897F2CE
  D669A23A EE47B92B B2BE942A 422DF4A5
  7ACB9433 BD17EC7A BB3721EC E7D1175F
  5C62BC58 C409F805 19691FBD FD925138
  quit
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
 no ip mroute-cache
!
interface BRI0
 ip address 12.12.12.13 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 dialer idle-timeout 99999
 dialer map ip 12.12.12.12 name lab-isdn 4724171
 dialer hold-queue 40
 dialer-group 1
 isdn spid1 919472411800 4724118
 isdn spid2 919472411901 4724119
 ppp authentication chap
 crypto map test
!
ip classless
ip route 0.0.0.0 0.0.0.0 12.12.12.12
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

lab-isdn1#

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

lab-isdn#write terminal
Building configuration...

Current configuration:
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname lab-isdn
!
enable secret 5 $1$oNe1$wDbhBdcN6x9Y5gfuMjqh10
!
username lab-isdn1 password 0 cisco
ip host ciscoca-ultra 171.69.54.46
ip host lab-isdn1 12.12.12.13
ip domain-name cisco.com
ip name-server 171.68.10.70
ip name-server 171.68.122.99
isdn switch-type basic-ni1
!
crypto ipsec transform-set mypolicy ah-sha-hmac
 esp-des esp-sha-hmac
!
crypto map test 10 ipsec-isakmp
 set peer 12.12.12.13
 set transform-set mypolicy
 match address 133
!
crypto ca identity lab
 enrollment url http://ciscoca-ultra
 crl optional
crypto ca certificate chain lab
 certificate 44FC6C531FC3446927E4EE307A806B20
  308201E0 3082018A A0030201 02021044
  FC6C531F C3446927 E4EE307A 806B2030
  0D06092A 864886F7 0D010104 05003042
  31163014 06035504 0A130D43 6973636F
  20537973 74656D73 3110300E 06035504
  0B130744 65767465 73743116 30140603
  55040313 0D434953 434F4341 2D554C54
  5241301E 170D3938 30343038 30303030
  30305A17 0D393930 34303832 33353935
  395A305A 31263024 06092A86 4886F70D
  01090216 17737461 6E6E6F75 732D6973
  646E2E63 6973636F 2E636F6D 311E301C
  060A2B06 0104012A 020B0201 130E3137
  312E3638 2E313137 2E313839 3110300E
  06035504 05130735 36373939 3139305C
  300D0609 2A864886 F70D0101 01050003
  4B003048 024100B8 F4A17A70 FAB5C2E3
  39186513 486779C7 61EF0AC1 3B6CFF83
  810E6D28 B3E4C034 CD803CFF 5158C270
  28FEBCDE CB6EF2D4 83BDD9B3 EAF915DB
  78266E96 500CD702 03010001 A3443042
  300B0603 551D0F04 04030205 20302806
  03551D11 0421301F 82177374 616E6E6F
  75732D69 73646E2E 63697363 6F2E636F
  6D8704AB 4475BD30 09060355 1D130402
  3000300D 06092A86 4886F70D 01010405
  00034100 BF65B931 0F960195 ABDD41D5
  622743D9 C12B5499 B3A8EB30 5005E6CC
  7FDF7C5B 51D13EB8 D46187E5 A1E7F711
  AEB7B33B AA4C6728 7A4BA692 00A44A05 C5CF973F
  quit
 certificate ca 3051DF7169BEE31B821DFE4B3A338E5F
  30820182 3082012C A0030201 02021030
  51DF7169 BEE31B82 1DFE4B3A 338E5F30
  0D06092A 864886F7 0D010104 05003042
  31163014 06035504 0A130D43 6973636F
  20537973 74656D73 3110300E 06035504
  0B130744 65767465 73743116 30140603
  55040313 0D434953 434F4341 2D554C54
  5241301E 170D3937 31323032 30313036
  32385A17 0D393831 32303230 31303632
  385A3042 31163014 06035504 0A130D43
  6973636F 20537973 74656D73 3110300E
  06035504 0B130744 65767465 73743116
  30140603 55040313 0D434953 434F4341
  2D554C54 5241305C 300D0609 2A864886
  F70D0101 01050003 4B003048 024100C1
  B69D7BF6 34E4EE28 A84E0DC6 FCA4DEA8
  04D89E50 C5EBE862 39D51890 D0D4B732
  678BDBF2 80801430 E5E56E7C C126E2DD
  DBE9695A DF8E5BA7 E67BAE87 29375302
  03010001 300D0609 2A864886 F70D0101
  04050003 410035AA 82B5A406 32489413
  A7FF9A9A E349E5B4 74615E05 058BA3CE
  7C5F00B4 019552A5 E892D2A3 86763A1F
  2852297F C68EECE1 F41E9A7B 2F38D02A
  B1D2F817 3F7B
  quit
 certificate 52A46D5D10B18A6F51E6BC735A36508C
  308201E0 3082018A A0030201 02021052
  A46D5D10 B18A6F51 E6BC735A 36508C30
  0D06092A 864886F7 0D010104 05003042
  31163014 06035504 0A130D43 6973636F
  20537973 74656D73 3110300E 06035504
  0B130744 65767465 73743116 30140603
  55040313 0D434953 434F4341 2D554C54
  5241301E 170D3938 30343038 30303030
  30305A17 0D393930 34303832 33353935
  395A305A 31263024 06092A86 4886F70D
  01090216 17737461 6E6E6F75 732D6973
  646E2E63 6973636F 2E636F6D 311E301C
  060A2B06 0104012A 020B0201 130E3137
  312E3638 2E313137 2E313839 3110300E
  06035504 05130735 36373939 3139305C
  300D0609 2A864886 F70D0101 01050003
  4B003048 024100D7 71AD5672 B487A019
  5ECD1954 6F919A3A 6270102E 5A9FF4DC
  7A608480 FB27A181 715335F4 399D3E57
  7F72B323 BF0620AB 60C371CF 4389BA4F
  C60EE6EA 21E06302 03010001 A3443042
  300B0603 551D0F04 04030207 80302806
  03551D11 0421301F 82177374 616E6E6F
  75732D69 73646E2E 63697363 6F2E636F
  6D8704AB 4475BD30 09060355 1D130402
  3000300D 06092A86 4886F70D 01010405
  00034100 8AD45375 54803CF3 013829A8
  8DB225A8 25342160 94546F3C 4094BBA3
  F2F5A378 97E2F06F DCFFC509 A07B930A
  FBE6C3CA E1FC7FD9 1E69B872 C402E62A A8814C09
  quit
!
interface Ethernet0
 ip address 20.20.20.20 255.255.255.0
!
interface BRI0
 description bri to rtp
 ip address 12.12.12.12 255.255.255.0
 no ip proxy-arp
 encapsulation ppp
 no ip mroute-cache
 bandwidth 128
 load-interval 30
 dialer idle-timeout 99999
 dialer hold-queue 40
 dialer-group 1
 isdn spid1 919472417100 4724171
 isdn spid2 919472417201 4724172
 ppp authentication chap
 crypto map test
!
ip classless
ip route 0.0.0.0 0.0.0.0 12.12.12.13
```

```
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

lab-isdn#

------------------ RSA-sig ---------------------------
lab-isdn#show debug
Cryptographic Subsystem:
  Crypto ISAKMP debugging is on
  Crypto Engine debugging is on
  Crypto IPSEC debugging is on
lab-isdn#

lab-isdn#
*Mar 21 20:16:50.871: ISAKMP (4): processing SA payload.
 message ID = 0
*Mar 21 20:16:50.871: ISAKMP (4): Checking ISAKMP transform 1
 against priority 65535
        policy
*Mar 21 20:16:50.875: ISAKMP: encryption DES-CBC
*Mar 21 20:16:50.875: ISAKMP: hash SHA
*Mar 21 20:16:50.875: ISAKMP: default group 1
*Mar 21 20:16:50.875: ISAKMP:  auth RSA sig
*Mar 21 20:16:50.879: ISAKMP (4): atts are acceptable.
 Next payload is 0
*Mar 21 20:16:50.879: Crypto engine 0: generate
 alg param

*Mar 21 20:16:54.070: CRYPTO_ENGINE: Dh phase 1
status: 0
*Mar 21 20:16:54.090: ISAKMP (4): SA is doing RSA
 signature authentication
*Mar 21 20:16:57.343: ISAKMP (4): processing KE
 payload. message ID = 0
*Mar 21 20:16:57.347: Crypto engine 0: generate alg param

*Mar 21 20:17:01.168: ISAKMP (4): processing NONCE
payload. message ID = 0
*Mar 21 20:17:01.176: Crypto engine 0: create ISAKMP
 SKEYID for conn id 4
*Mar 21 20:17:01.188: ISAKMP (4): SKEYID state generated
*Mar 21 20:17:07.331: ISAKMP (4): processing ID
 payload. message ID = 0
*Mar 21 20:17:07.331: ISAKMP (4): processing CERT
 payload. message ID = 0
*Mar 21 20:17:07.497: ISAKMP (4): cert approved
 with warning
*Mar 21 20:17:07.600: ISAKMP (4): processing SIG
 payload. message ID = 0
*Mar 21 20:17:07.608: Crypto engine 0: RSA decrypt
 with public key
*Mar 21 20:17:07.759: generate hmac context for
 conn id 4
*Mar 21 20:17:07.767: ISAKMP (4): SA has been
 authenticated
```

```
*Mar 21 20:17:07.775: generate hmac context for
 conn id 4
*Mar 21 20:17:07.783: Crypto engine 0: RSA encrypt
 with private key
*Mar 21 20:17:08.672: CRYPTO_ENGINE: key process
 suspended and continued
*Mar 21 20:17:08.878: CRYPTO_ENGINE: key process
 suspended and continued
*Mar 21 20:17:09.088: CRYPTO_ENGINE: key process
 suspended and continued
*Mar 21 20:17:09.291: CRYPTO_ENGINE: key process
 suspended and continued
*Mar 21 20:17:09.493: CRYPTO_ENGINE: key process
 suspended and continued
*Mar 21 20:17:09.795: CRYPTO_ENGINE: key process
 suspended and continued
*Mar 21 20:17:10.973: generate hmac context for
 conn id 4
*Mar 21 20:17:10.981: ISAKMP (4): processing SA
 payload. message ID = -538880964
*Mar 21 20:17:10.981: ISAKMP (4): Checking IPSec proposal 1
*Mar 21 20:17:10.981: ISAKMP: transform 1, AH_SHA_HMAC
*Mar 21 20:17:10.985: ISAKMP: attributes in transform:
*Mar 21 20:17:10.985: ISAKMP: encaps is 1
*Mar 21 20:17:10.985: ISAKMP: SA life type in seconds
*Mar 21 20:17:10.985: ISAKMP: SA life duration (basic) of 3600
*Mar 21 20:17:10.989: ISAKMP: SA life type in kilobytes
*Mar 21 20:17:10.989: ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar 21 20:17:10.993: ISAKMP (4): atts are acceptable.
*Mar 21 20:17:10.993: ISAKMP (4): Checking IPSec proposal 1
*Mar 21 20:17:10.993: ISAKMP: transform 1, ESP_DES
*Mar 21 20:17:10.997: ISAKMP: attributes in transform:
*Mar 21 20:17:10.997: ISAKMP: encaps is 1
*Mar 21 20:17:10.997: ISAKMP: SA life type in seconds
*Mar 21 20:17:10.997: ISAKMP: SA life duration (basic) of 3600
*Mar 21 20:17:11.001: ISAKMP: SA life type in kilobytes
*Mar 21 20:17:11.001: ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar 21 20:17:11.001: ISAKMP: HMAC algorithm is SHA
*Mar 21 20:17:11.005: ISAKMP (4): atts are acceptable.
*Mar 21 20:17:11.005: IPSEC(validate_proposal_request):
 proposal part #1,
  (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13,
    dest_proxy= 20.20.20.0/0.0.0.0/0/0,
    src_proxy= 40.40.40.0/0.0.0.16/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar 21 20:17:11.013: IPSEC(validate_proposal_request):
 proposal part #2,
  (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13,
    dest_proxy= 20.20.20.0/0.0.0.0/0/0,
    src_proxy= 40.40.40.0/0.0.0.16/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar 21 20:17:11.021: ISAKMP (4): processing NONCE payload.
  message ID = -538880964
*Mar 21 20:17:11.021: ISAKMP (4): processing ID payload.
  message ID = -538880964
*Mar 21 20:17:11.021: ISAKMP (4): processing ID payload.
 message ID = -538880964
*Mar 21 20:17:11.025: IPSEC(key_engine):
```

```
got a queue event...
*Mar 21 20:17:11.029: IPSEC(spi_response):
getting spi 112207019 for SA
        from 12.12.12.13     to 12.12.12.12 for prot 2
*Mar 21 20:17:11.033: IPSEC(spi_response):
getting spi 425268832 for SA
        from 12.12.12.13     to 12.12.12.12 for prot 3
*Mar 21 20:17:11.279: generate hmac context for conn id 4
*Mar 21 20:17:11.612: generate hmac context for conn id 4
*Mar 21 20:17:11.644: ISAKMP (4): Creating IPSec SAs
*Mar 21 20:17:11.644:         inbound SA from
12.12.12.13 to 12.12.12.12
        (proxy 40.40.40.0      to 20.20.20.0     )
*Mar 21 20:17:11.648:         has spi 112207019
and conn_id 5 and flags 4
*Mar 21 20:17:11.648:         lifetime of 3600 seconds
*Mar 21 20:17:11.648:         lifetime of 4608000 kilobytes
*Mar 21 20:17:11.652: outbound SA from 12.12.12.12 to 12.12.12.13
        (proxy 20.20.20.0  to 40.40.40.0     )
*Mar 21 20:17:11.652: has spi 83231845 and conn_id 6 and flags 4
*Mar 21 20:17:11.656: lifetime of 3600 seconds
*Mar 21 20:17:11.656: lifetime of 4608000 kilobytes
*Mar 21 20:17:11.656: ISAKMP (4): Creating IPSec SAs
*Mar 21 20:17:11.656:  inbound SA from 12.12.12.13 to 12.12.12.12
        (proxy 40.40.40.0      to 20.20.20.0     )
*Mar 21 20:17:11.660: has spi 425268832 and conn_id 7 and flags 4
*Mar 21 20:17:11.660: lifetime of 3600 seconds
*Mar 21 20:17:11.664: lifetime of 4608000 kilobytes
*Mar 21 20:17:11.664: outbound SA from 12.12.12.12 to 12.12.12.13
        (proxy 20.20.20.0 to 40.40.40.0     )
*Mar 21 20:17:11.668: has spi 556010247 and conn_id 8 and flags 4
*Mar 21 20:17:11.668: lifetime of 3600 seconds
*Mar 21 20:17:11.668: lifetime of 4608000 kilobytes
*Mar 21 20:17:11.676: IPSEC(key_engine): got a queue event...
*Mar 21 20:17:11.676: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13,
    dest_proxy= 20.20.20.0/255.255.255.0/0/0,
    src_proxy= 40.40.40.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x6B024AB(112207019), conn_id= 5, keysize= 0, flags= 0x4
*Mar 21 20:17:11.680: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.12.12.12, dest= 12.12.12.13,
    src_proxy= 20.20.20.0/255.255.255.0/0/0,
    dest_proxy= 40.40.40.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x4F60465(83231845), conn_id= 6, keysize= 0, flags= 0x4
*Mar 21 20:17:11.687: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13,
    dest_proxy= 20.20.20.0/255.255.255.0/0/0,
    src_proxy= 40.40.40.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x19591660(425268832), conn_id= 7, keysize= 0, flags= 0x4
*Mar 21 20:17:11.691: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.12.12.12, dest= 12.12.12.13,
    src_proxy= 20.20.20.0/255.255.255.0/0/0,
    dest_proxy= 40.40.40.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x21240B07(556010247), conn_id= 8, keysize= 0, flags= 0x4
*Mar 21 20:17:11.699: IPSEC(create_sa): sa created,
  (sa) sa_dest= 12.12.12.12, sa_prot= 51,
    sa_spi= 0x6B024AB(112207019),
    sa_trans= ah-sha-hmac , sa_conn_id= 5
*Mar 21 20:17:11.703: IPSEC(create_sa): sa created,
  (sa) sa_dest= 12.12.12.13, sa_prot= 51,
    sa_spi= 0x4F60465(83231845),
    sa_trans= ah-sha-hmac , sa_conn_id= 6
*Mar 21 20:17:11.707: IPSEC(create_sa): sa created,
  (sa) sa_dest= 12.12.12.12, sa_prot= 50,
    sa_spi= 0x19591660(425268832),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 7
*Mar 21 20:17:11.707: IPSEC(create_sa): sa created,
  (sa) sa_dest= 12.12.12.13, sa_prot= 50,
    sa_spi= 0x21240B07(556010247),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 8
*Mar 21 20:18:06.767: ISADB: reaper checking SA, conn_id = 4
lab-isdn#
```

IPSec和ISAKMP故障排除

通常，最好使用以下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	
debug crypto pki trans	* debug crypto ipsec
* debug crypto isakmp	debug crypto key
debug crypto sess	debug crypto engine
show crypto engine connections active	show crypto engine connections dropped-packet
show crypto engine configuration	* show crypto ca certificates
* show crypto key mypubkey rsa	* show crypto key pubkey-chain rsa
show crypto isakmp policy	show crypto isakmp sa
show crypto ipsec sa	show crypto ipsec session-key
show crypto ipsec transform-proposal	show crypto map interface bri 0
show crypto map tag test	clear crypto connection <connection id of SA>
* clear crypto isakmp	* clear crypto sa
clear crypto sa counters	clear crypto sa map
clear crypto sa peer	clear crypto sa spi
clear crypto sa counters	

以下顯示其中一些命令的輸出示例。

```
wan2511#show crypto engine connections active
ID     Interface        IP-Address  State  Algorithm       Encrypt  Decrypt
```

```
 9    Serial0         20.20.20.21 set    HMAC_SHA        0        240
 10   Serial0         20.20.20.21 set    HMAC_SHA        240      0

wan2511#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

wan2511#show crypto engine configuration
slot:               0
engine name:        unknown
engine type:        software
serial number:      01496536
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    140
input queue bot:    140
input queue count:  0

wan2511#show crypto key mypubkey rsa
% Key pair was generated at: 00:09:04 UTC Mar 1 1993
Key name: wan2511.cisco.com
Usage:    General Purpose Key
Key Data:
 305C300D 06092A86 4886F70D 01010105
00034B00 30480241 00E9007B E5CD7DC8
 6E1C0423 92044254 92C972AD 0CCE9796
86797EAA B6C4EFF0 0F0A5378 6AFAE43B
 3A2BD92F 98039DAC 08741E82 5D9053C4
D9CFABC1 AB54E0E2 BB020301 0001

wan2511#show crypto key pubkey-chain rsa
wan2511#

wan2511#show crypto isakmp policy
Protection suite of priority 1
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               240 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
wan2511#show crypto isakmp sa
    dst           src          state        conn-id   slot
20.20.20.21    20.20.20.20    QM_IDLE           7       0

wan2511#
wan2511#show crypto ipsec sa

interface: Serial0
    Crypto map tag: test, local addr. 20.20.20.21

   local  ident (addr/mask/prot/port): (50.50.50.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (60.60.60.0/255.255.255.0/0/0)
   current_peer: 20.20.20.20
     PERMIT, flags={origin_is_acl,ident_is_ipsec,}
    #pkts encaps: 320, #pkts encrypt: 320, #pkts digest 320
    #pkts decaps: 320, #pkts decrypt: 320, #pkts verify 320
    #send errors 0, #recv errors 0
```

```
     local crypto endpt.: 20.20.20.21, remote crypto endpt.: 20.20.20.20
     path mtu 1500, media mtu 1500
     current outbound spi: 6625CD

     inbound esp sas:
      spi: 0x1925112F(421859631)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607971/3354)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:
      spi: 0x12050DD2(302321106)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 9, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607958/3354)
        replay detection support: Y


     outbound esp sas:
      spi: 0x3262313(52830995)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 12, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607971/3354)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:
      spi: 0x6625CD(6694349)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 10, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607958/3354)
        replay detection support: Y

wan2511#show crypto ipsec session-key
Session key lifetime: 4608000 kilobytes/3600 seconds

wan2511#show crypto ipsec transform-proposal
Transform proposal auth2: { ah-sha-hmac  }
   supported settings = { Tunnel,  },
   default settings = { Tunnel,  },
   will negotiate = { Tunnel,  },

   { esp-des esp-sha-hmac  }
   supported settings = { Tunnel,  },
   default settings = { Tunnel,  },
   will negotiate = { Tunnel,  },


wan2511#show crypto map interface serial 0
Crypto Map "test" 10 ipsec-isakmp
        Peer = 20.20.20.20
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 50.50.50.0/0.0.0.255
                dest:   addr = 60.60.60.0/0.0.0.255
        Current peer: 20.20.20.20
        Session key lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform proposals={ auth2, }

wan2511#show crypto map tag test
Crypto Map "test" 10 ipsec-isakmp
        Peer = 20.20.20.20
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 50.50.50.0/0.0.0.255
                dest:   addr = 60.60.60.0/0.0.0.255
        Current peer: 20.20.20.20
        Session key lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform proposals={ auth2, }

wan2511#

----------------------
lab-isdn1#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 5    BRI0            12.12.12.13 set    HMAC_SHA        0        89
 6    BRI0            12.12.12.13 set    HMAC_SHA        89       0

lab-isdn1#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

BRI0                 12.12.12.13   4
lab-isdn1#show crypto engine configuration
slot:               0
engine name:        unknown
engine type:        software
serial number:      05679987
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    243
input queue bot:    243
input queue count:  0

lab-isdn1#show crypto ca cert
Certificate
  Subject Name
    Name: lab-isdn1.cisco.com
    Serial Number: 05679987
  Status: Available
  Certificate Serial Number: 3E1ED472BDA2CE0163FB6B0B004E5EEE
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F
  Key Usage: Not Set

Certificate
  Subject Name
    Name: lab-isdn1.cisco.com
    Serial Number: 05679987
  Status: Available
  Certificate Serial Number: 503968D890F7D409475B7280162754D2
  Key Usage: Signature
```

```
lab-isdn1#show crypto key mypubkey rsa
% Key pair was generated at: 03:10:23 UTC Mar 21 1993
Key name: lab-isdn1.cisco.com
Usage:    Signature Key
Key Data:
 305C300D 06092A86 4886F70D 01010105
00034B00 30480241 00BECE2D 8CB32E6B
 090ADE0D 46AF8D4A 1F378500 3435D0C7
293BF915 180C9E4C F81A6A43 AEE4F046
 87B8E285 9D33D5CE 042E5DDE A63DA54A
312AD425 5A756014 CB020301 0001
% Key pair was generated at: 03:11:17 UTC Mar 21 1993
Key name: lab-isdn1.cisco.com
Usage:    Encryption Key
Key Data:
 305C300D 06092A86 4886F70D 01010105
00034B00 30480241 00D2D125 FFBBFC6E
 5693CB43 855473C1 65BC7CCA F645C35B
ED554BAA 0B119AFA 6F0853F5 745E0B84
 922E39B5 FA84C4DD 05C19AA6 25818439
5C6CBC7F A4614F61 77020301 0001

lab-isdn1#show crypto key pubkey-chain rsa
Key name: Cisco SystemsDevtestCISCOCA-ULTRA
Key serial number: C7040262
Key usage: signatures only
Key source: certificate
Key data:
 305C300D 06092A86 4886F70D 01010105
 00034B00 30480241 00C1B69D 7BF634E4
 EE28A84E 0DC6FCA4 DEA804D8 9E50C5EB
 E86239D5 1890D0D4 B732678B DBF28080
 1430E5E5 6E7CC126 E2DDDBE9 695ADF8E
 5BA7E67B AE872937 53020301 0001

Key name: lab-isdn.cisco.com
Key address: 171.68.117.189
Key serial number: 05679919
Key usage: general purpose
Key source: certificate
Key data:
 305C300D 06092A86 4886F70D 01010105
00034B00 30480241 00D771AD 5672B487
 A0195ECD 19546F91 9A3A6270 102E5A9F
F4DC7A60 8480FB27 A1817153 35F4399D
 3E577F72 B323BF06 20AB60C3 71CF4389
 BA4FC60E E6EA21E0 63020301 0001


lab-isdn1#show crypto isakmp policy
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit


lab-isdn1#show crypto isakmp sa
    dst           src          state        conn-id   slot
12.12.12.12    12.12.12.13    QM_IDLE           4       0
```

```
lab-isdn1#show crypto ipsec sa

interface: BRI0
    Crypto map tag: test, local addr. 12.12.12.13

   local  ident (addr/mask/prot/port): (40.40.40.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
   current_peer: 12.12.12.12
     PERMIT, flags={origin_is_acl,ident_is_ipsec,}
    #pkts encaps: 89, #pkts encrypt: 89, #pkts digest 89
    #pkts decaps: 89, #pkts decrypt: 89, #pkts verify 89
    #send errors 11, #recv errors 0

     local crypto endpt.: 12.12.12.13, remote crypto endpt.: 12.12.12.12
     path mtu 1500, media mtu 1500
     current outbound spi: 6B024AB

     inbound esp sas:
      spi: 0x21240B07(556010247)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 7, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607989/3062)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:
      spi: 0x4F60465(83231845)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607984/3062)
        replay detection support: Y


     outbound esp sas:
      spi: 0x19591660(425268832)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 8, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607989/3062)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:
      spi: 0x6B024AB(112207019)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 6, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607984/3062)
        replay detection support: Y


lab-isdn1#show crypto ipsec session-key
Session key lifetime: 4608000 kilobytes/3600 seconds


lab-isdn1#show crypto ipsec transform-proposal
Transform proposal mypolicy: { ah-sha-hmac  }
   supported settings = { Tunnel,  },
   default settings = { Tunnel,  },
   will negotiate = { Tunnel,  },
   { esp-des esp-sha-hmac  }
   supported settings = { Tunnel,  },
   default settings = { Tunnel,  },
   will negotiate = { Tunnel,  },


lab-isdn1#show crypto map interface bri 0
Crypto Map "test" 10 ipsec-isakmp
        Peer = 12.12.12.12
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 20.20.20.0/0.0.0.255
        Current peer: 12.12.12.12
        Session key lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform proposals={ mypolicy, }


lab-isdn1#show crypto map tag test
Crypto Map "test" 10 ipsec-isakmp
        Peer = 12.12.12.12
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 20.20.20.0/0.0.0.255
        Current peer: 12.12.12.12
        Session key lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform proposals={ mypolicy, }

lab-isdn1#

----------------------------
lab-isdn1#clear crypto isakmp
lab-isdn1#
*Mar 21 20:58:34.503: ISADB: reaper checking SA, conn_id = 4  DELETE IT!
*Mar 21 20:58:34.507: generate hmac context for conn id 4
*Mar 21 20:58:34.519: CRYPTO(epa_release_crypto_conn_entry): released conn 4
lab-isdn1#
lab-isdn1#clear crypto sa
lab-isdn1#
*Mar 21 20:58:42.495: IPSEC(delete_sa): deleting SA,
  (sa) sa_dest= 12.12.12.13, sa_prot= 51,
    sa_spi= 0x4F60465(83231845),
    sa_trans= ah-sha-hmac , sa_conn_id= 5
*Mar 21 20:58:42.499: CRYPTO(epa_release_crypto_conn_entry): released conn 5
*Mar 21 20:58:42.499: IPSEC(delete_sa): deleting SA,
  (sa) sa_dest= 12.12.12.12, sa_prot= 51,
    sa_spi= 0x6B024AB(112207019),
    sa_trans= ah-sha-hmac , sa_conn_id= 6
*Mar 21 20:58:42.503: CRYPTO(epa_release_crypto_conn_entry): released conn 6
*Mar 21 20:58:42.503: IPSEC(delete_sa): deleting SA,
  (sa) sa_dest= 12.12.12.13, sa_prot= 50,
    sa_spi= 0x21240B07(556010247),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 7
*Mar 21 20:58:42.507: CRYPTO(epa_release_crypto_conn_entry): released conn 7
*Mar 21 20:58:42.507: IPSEC(delete_sa): deleting SA,
  (sa) sa_dest= 12.12.12.12, sa_prot= 50,
    sa_spi= 0x19591660(425268832),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 8
*Mar 21 20:58:42.511: CRYPTO(epa_release_crypto_conn_entry): released conn 8
lab-isdn1#
```

相關資訊

- 思科網路層加密配置和故障排除：背景 — 第1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