IPSec Over Cable組態和偵錯範例

目錄

簡介

Internet協定安全(IPsec)是一個開放式標準框架，可確保通過IP網路進行安全的專用通訊。根據Internet工程任務組(IETF)制定的標準，IPsec可確保公共IP網路中資料通訊的機密性、完整性和真實性。IPsec為基於標準的靈活解決方案提供了部署網路範圍安全策略的必要元件。

本檔案將提供兩個Cisco纜線資料機之間的IPsec組態範例。此組態會透過兩個Cisco uBR9xx系列纜線資料機路由器之間的纜線網路建立加密通道。兩個網路之間的所有流量都會進行加密。但是傳送到其他網路的流量會允許以未加密的方式通過。對於小型辦公室、家庭辦公室(SOHO)使用者，這允許通過有線網路建立虛擬專用網路(VPN)。

必要條件

需求

本文件沒有特定需求。

採用元件

數據機必須符合以下要求才能在兩個電纜數據機上配置IPsec:

- 在路由模式下的Cisco uBR904、uBR905或uBR924
- IPsec 56功能集
- Cisco IOS®軟體版本12.0(5)T或更新版本

此外，您必須擁有纜線資料機終端系統(CMTS)，這是任何符合有線電纜資料服務介面規範(DOCSIS)的前端纜線路由器，例如Cisco uBR7246、Cisco uBR7223或Cisco uBR7246VXR。

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。

背景理論

本檔案中的範例使用uBR904纜線資料機、uBR924纜線資料機和uBR7246VXR CMTS。纜線資料機執行Cisco IOS軟體版本12.1(6)，而CMTS執行Cisco IOS軟體版本12.1(4)EC。

註：此示例是通過控制檯埠對電纜數據機進行手動配置完成的。如果通過DOCSIS配置檔案執行自動進程（使用IPsec配置建立ios.cfg指令碼），則不能使用訪問清單100*和*101。這是因為簡單網路管理協定(SNMP)的Cisco實施使用Cisco IOS訪問清單。它為每個介面建立一個訪問清單。在uBR904、924和905上，通常使用前兩個存取清單（100和101）。 在支援通用串列匯流排(USB)的電纜數據機上（如CVA120），使用三個訪問清單（100、101和102）。

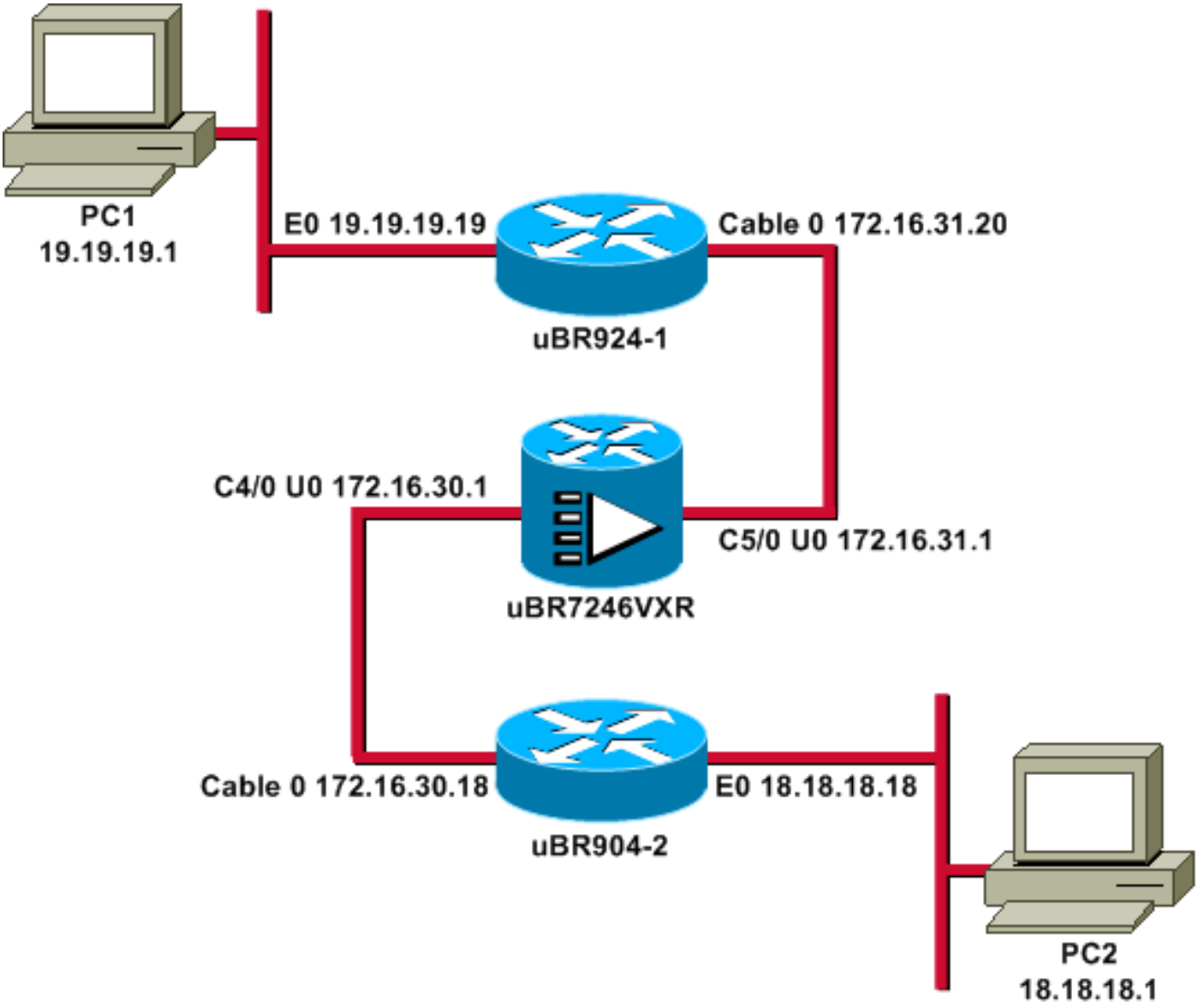
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)查詢有關本文檔中的命令的其他資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此圖中的所有IP地址都具有24位掩碼。

組態

本檔案會使用以下設定：

- uBR924-1
- uBR904-2
- uBR7246VXR

uBR924-1

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ubr924-1
!
enable password ww
!
!
!
```

```
!
clock timezone - -8
ip subnet-zero
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
!
crypto isakmp policy 10
!--- Creates an Internet Key Exchange (IKE) policy with
the specified priority !--- number of 10. The range for
the priority is 1 to 10000, where 1 is the !--- highest
priority. This command also enters Internet Security
Association !--- and Key Management Protocol (ISAKMP)
policy configuration command mode. hash md5
!--- Specifies the MD5 (HMAC variant) hash algorithm for
packet authentication. authentication pre-share
!--- Specifies that the authentication keys are pre-
shared, as opposed to !--- dynamically negotiated using
Rivest, Shamir, and Adelman (RSA) public !--- key
signatures. group 2
!--- Diffie-Hellman group for key negotiation. lifetime
3600
!--- Defines how long, in seconds, each security
association should exist before !--- it expires. Its
range is 60 to 86400, and in this case, it is 1 hour.
crypto isakmp key mykey address 18.18.18.18
!--- Specifies the pre-shared key that should be used
with the peer at the !--- specific IP address. The key
can be any arbitrary alphanumeric key up to !--- 128
characters. The key is case-sensitive and must be
entered identically !--- on both routers. In this case,
the key is mykey and the peer is the !--- Ethernet
address of uBR904-2
.
!
crypto IPSec transform-set TUNNELSET ah-md5-hmac esp-des
!--- Establishes the transform set to use for IPsec
encryption. As many as !--- three transformations can be
specified for a set. Authentication Header !--- and ESP
are in use. Another common transform set used in
industry is !--- esp-des esp-md5-hmac.

!
crypto map MYMAP local-address Ethernet0
!--- Creates the MYMAP crypto map and applies it to the
Ethernet0 interface.

crypto map MYMAP 10 ipsec-isakmp
!--- Creates a crypto map numbered 10 and enters crypto
map configuration mode. set peer 18.18.18.18
!--- Identifies the IP address for the destination peer
router. In this case, !--- the Ethernet interface of the
remote cable modem (ubr904-2) is used. set transform-set
TUNNELSET
!--- Sets the crypto map to use the transform set
previously created. match address 101
!--- Sets the crypto map to use the access list that
specifies the type of !--- traffic to be encrypted. !---
Do not use access lists 100, 101, and 102 if the IPsec
config is !--- downloaded through the ios.cfg in the
DOCSIS configuration file.
```

```
!
!
!
!
voice-port 0
 input gain -2
 output attenuation 0
!
voice-port 1
 input gain -2
 output attenuation 0
!
!
!
interface Ethernet0
 ip address 19.19.19.19 255.255.255.0
 ip rip send version 2
 ip rip receive version 2
 no ip route-cache
 no ip mroute-cache
!
interface cable-modem0
 ip rip send version 2
 ip rip receive version 2
 no ip route-cache
 no ip mroute-cache
 cable-modem downstream saved channel 525000000 39 1
 cable-modem mac-timer t2 40000
 no cable-modem compliant bridge
 crypto map MYMAP
!--- Applies the previously created crypto map to the
cable interface. ! router rip version 2 network 19.0.0.0
network 172.16.0.0 ! ip default-gateway 172.16.31.1 ip
classless ip http server ! access-list 101 permit ip
19.19.19.0 0.0.0.255 18.18.18.0 0.0.0.255
!--- Access list that identifies the traffic to be
encrypted. In this case, !--- it is setting traffic from
the local Ethernet network to the remote !--- Ethernet
network. snmp-server manager ! line con 0 transport
input none line vty 0 4 password ww login ! end
```

另一個電纜數據機的配置非常相似，因此省略了先前配置中的大多數註釋。

uBR904-2

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ubr904-2
!
enable password ww
!
!
!
!
!
clock timezone - -8
ip subnet-zero
no ip finger
```

```
!
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
 group 2
 lifetime 3600
crypto isakmp key mykey address 19.19.19.19
!
!
crypto IPSec transform-set TUNNELSET ah-md5-hmac ESP-Des
!
crypto map MYMAP local-address Ethernet0
crypto map MYMAP 10 ipsec-isakmp
 set peer 19.19.19.19
!--- Identifies the IP address for the destination peer
router. In this case, !--- the Ethernet interface of the
remote cable modem (uBR924-1) is used. set transform-set
TUNNELSET
 match address 101
!
!
!
!
interface Ethernet0
 ip address 18.18.18.18 255.255.255.0
 ip rip send version 2
 ip rip receive version 2
!
interface cable-modem0
 ip rip send version 2
 ip rip receive version 2
 no keepalive
 cable-modem downstream saved channel 555000000 42 1
 cable-modem Mac-timer t2 40000
 no cable-modem compliant bridge
 crypto map MYMAP
!
router rip
 version 2
 network 18.0.0.0
 network 172.16.0.0
!
ip default-gateway 172.16.30.1
ip classless
no ip http server
!
access-list 101 permit ip 18.18.18.0 0.0.0.255
19.19.19.0 0.0.0.255
snmp-server manager
!
line con 0
 transport input none
line vty 0 4
 password ww
 login
!
end
```

CMTS uBR7246VXR還運行路由資訊協定(RIP)第2版，以便路由正常工作。以下是CMTS上使用的RIP配置：

uBR7246VXR
router rip version 2 network 172.16.0.0 no auto-summary

驗證

使用本節內容，確認您的組態是否正常運作。

若要確認IPsec是否運作：

- 驗證以下內容：Cisco IOS軟體支援IPsec。運行配置正確。介面已開啟。路由工作正常。為加密流量定義的訪問清單正確。
- 建立流量並檢視加密和解密，以檢視增加的流量。
- 開啟加密的調試。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

對兩個纜線資料機發出show version指令。

```
ubr924-1#show version
Cisco Internetwork Operating System Software
IOS (tm) 920 Software (UBR920-K1O3SV4Y556I-M), Version 12.1(6),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Wed 27-Dec-00 16:36 by kellythw
Image text-base: 0x800100A0, data-base: 0x806C1C20

ROM: System Bootstrap, Version 12.0(6r)T3, RELEASE SOFTWARE (fc1)

ubr924-1 uptime is 1 hour, 47 minutes
System returned to ROM by reload at 10:39:05 - Fri Feb 9 2001
System restarted at 10:40:05 - Fri Feb 9 2001
System image file is "flash:ubr920-k1o3sv4y556i-mz.121-6"

cisco uBR920 CM (MPC850) processor (revision 3.e)
with 15872K/1024K bytes of memory.
Processor board ID FAA0422Q04F
Bridging software.
1 Ethernet/IEEE 802.3 interface(s)
1 Cable Modem network interface(s)
3968K bytes of processor board System flash (Read/Write)
1536K bytes of processor board Boot flash (Read/Write)

Configuration register is 0x2102
```

uBR924-1運行Cisco IOS軟體版本12.1(6)和VALUE SMALL OFFICE/VOICE/FW IPSec 56功能集。

```
ubr904-2#show version
Cisco Internetwork Operating System Software
IOS (TM) 900 Software (UBR900-K1OY556I-M), Version 12.1(6),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Wed 27-DEC-00 11:06 by kellythw
```

```
Image text-base: 0x08004000, database: 0x085714DC

ROM: System Bootstrap, Version 11.2(19980518:195057), RELEASED SOFTWARE
ROM: 900 Software (UBR900-RBOOT-M), Version 11.3(11)NA,
EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)

ubr904-2 uptime is 1 hour, 48 minutes
System returned to ROM by reload at 10:38:44 - Fri Feb 9 2001
System restarted at 10:40:37 - Fri Feb 9 2001
System image file is "flash:ubr900-k1oy556i-mz.121-6"

cisco uBR900 CM (68360) processor (revision D)
with 8192K bytes of memory.
Processor board ID FAA0235Q0ZS
Bridging software.
1 Ethernet/IEEE 802.3 interface(s)
1 Cable Modem network interface(s)
4096K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Boot flash (Read/Write)

Configuration register is 0x2102
```

uBR904-2運行帶有SMALL OFFICE/FW IPSec 56功能集的Cisco IOS軟體版本12.1(6)。

```
ubr924-1#show ip interface brief
Interface              IP-Address      OK? Method Status          Protocol
Ethernet0              19.19.19.19     YES NVRAM  up              up
cable-modem0           172.16.31.20    YES unset  up              up

ubr904-2#show ip interface brief
Interface              IP-Address      OK? Method Status          Protocol
Ethernet0              18.18.18.18     YES NVRAM  up              up
cable-modem0           172.16.30.18    YES unset  up              up
```

從最後一個命令中，您可以看到乙太網介面已啟動。已手動輸入乙太網介面的IP地址。電纜介面也已開啟，它們通過DHCP獲取其IP地址。由於這些纜線地址是動態分配的，因此它們不能用作IPSec配置中的對等體。

```
ubr924-1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - ISIS level-1, L2 - ISIS level-2, ia - ISIS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.31.1 to network 0.0.0.0

     19.0.0.0/24 is subnetted, 1 subnets
C       19.19.19.0 is directly connected, Ethernet0
R    18.0.0.0/8 [120/2] via 172.16.31.1, 00:00:23, cable-modem0
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
R       172.16.135.0/25 [120/1] via 172.16.31.1, 00:00:23, cable-modem0
R       172.16.29.0/27 [120/1] via 172.16.31.1, 00:00:23, cable-modem0
R       172.16.30.0/24 [120/1] via 172.16.31.1, 00:00:23, cable-modem0
C       172.16.31.0/24 is directly connected, cable-modem0
R    192.168.99.0/24 [120/3] via 172.16.31.1, 00:00:24, cable-modem0
     10.0.0.0/24 is subnetted, 2 subnets
R       10.10.10.0 [120/2] via 172.16.31.1, 00:00:24, cable-modem0
S*   0.0.0.0/0 [1/0] via 172.16.31.1
```

從該輸出中可以看到，uBR924-1正在學習路由18.18.18.0，該路由是uBR904-2的乙太網介面。

```
ubr904-2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - ISIS, L1 - ISIS level-1, L2 - ISIS level-2, IA - ISIS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.30.1 to network 0.0.0.0

R    19.0.0.0/8 [120/2] via 172.16.30.1, 00:00:17, cable-modem0
     18.0.0.0/24 is subnetted, 1 subnets
C       18.18.18.0 is directly connected, Ethernet0
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
R       172.16.135.0/25 [120/1] via 172.16.30.1, 00:00:17, cable-modem0
R       172.16.29.224/27 [120/1] via 172.16.30.1, 00:00:17, cable-modem0
C       172.16.30.0/24 is directly connected, cable-modem0
R       172.16.31.0/24 [120/1] via 172.16.30.1, 00:00:17, cable-modem0
R    192.168.99.0/24 [120/3] via 172.16.30.1, 00:00:18, cable-modem0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.10.10.0 [120/2] via 172.16.30.1, 00:00:18, cable-modem0
S*   0.0.0.0/0 [1/0] via 172.16.30.1
```

從uBR904-2的路由表中，可以看到uBR924-1的乙太網路位於路由表中。

注意：在某些情況下，您無法在兩個纜線資料機之間執行路由通訊協定。在這種情況下，您必須在CMTS上新增靜態路由，以便為纜線資料機的乙太網介面定向流量。

接下來要檢查的是訪問清單的認證；在兩台路由器上發出**show access-lists**命令。

```
ubr924-1#show access-lists
Extended IP access list 101
    permit ip 19.19.19.0 0.0.0.255 18.18.18.0 0.0.0.255 (2045 matches)

ubr904-2#show access-lists
Extended IP access list 101
    permit ip 18.18.18.0 0.0.0.255 19.19.19.0 0.0.0.255 (2059 matches)
```

當位於uBR924-1(19.19.19.0)後面的LAN將IP流量傳送到uBR904-2(18.18.18.0)後面的LAN時，存取清單會設定IPsec作業階段，反之亦然。請勿在存取清單上使用「*any*」，因為它會建立問題。有關詳細資訊，請參閱配置IPsec網路安全。

沒有IPsec流量。發出**show crypto engine connection active**命令。

```
ubr924-1#show crypto engine connection active
ID Interface    IP-Address    State    Algorithm           Encrypt  Decrypt
1                              set     HMAC_MD5+DES_56_CB        0        0

ubr904-2#show crypto engine connection active
ID Interface    IP-Address    State    Algorithm           Encrypt  Decrypt
1                              set     HMAC_MD5+DES_56_CB        0        0
```

沒有IPsec連線，因為沒有與訪問清單匹配的流量。

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

下一步是開啟一些加密偵錯以生成相關流量。

在此範例中，以下偵錯處於開啟狀態：

- debug crypto engine
- debug crypto IPsec
- debug crypto key-exchange
- debug crypto isakmp

您必須首先生成一些有趣的流量才能看到調試的輸出。從uBR904-2的乙太網埠向uBR924-1（IP地址19.19.1）上的PC發出擴展ping。

```
ubr904-2#ping ip
Target IP address: 19.19.19.1
!--- IP address of PC1 behind the Ethernet of uBR924-1. Repeat count [5]: 100
!--- Sends 100 pings. Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y
Source address or interface: 18.18.18.18
!--- IP address of the Ethernet behind uBR904-2. Type of service [0]: Set DF bit in IP header?
[no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp,
Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 100, 100-byte
ICMP Echos to 19.19.19.1, timeout is 2 seconds:
```

uBR924-2顯示以下調試輸出：

```
ubr904-2#
01:50:37: IPSec(sa_request): ,
 (key eng. msg.) src= 18.18.18.18, dest= 19.19.19.19,
    src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4),
    protocol= AH, transform= ah-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x19911A16(428939798), conn_id= 0, keysize= 0, flags= 0x4004
01:50:37: IPSec(sa_request): ,
  (key Eng. msg.) src= 18.18.18.18, dest= 19.19.19.19,
    src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= ESP-Des ,
    lifedur= 3600s and 4608000kb,
    spi= 0x7091981(118036865), conn_id= 0, keysize= 0, flags= 0x4004
01:50:37: ISAKMP: received ke message (1/2)
01:50:37: ISAKMP (0:1): sitting IDLE. Starting QM immediately (QM_IDLE)
01:50:37: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1108017901
01:50:37: CryptoEngine0: generate hmac context for conn id 1
01:50:37: ISAKMP (1): sending packet to 19.19.19.19 (I) QM_IDLE
01:50:37: ISAKMP (1): received packet from 19.19.19.19 (I) QM_IDLE
01:50:37: CryptoEngine0: generate hmac context for conn id 1
01:50:37: ISAKMP (0:1): processing SA payload. message ID = 1108017901
01:50:37: ISAKMP (0:1): Checking IPSec proposal 1
01:50:37: ISAKMP: transform 1, AH_MD5
01:50:37: ISAKMP:   attributes in transform:
01:50:3.!!!!!!!!!!!!!!!!!!!!!!!7: ISAKMP:      encaps is 1
01:50:37: ISAKMP:      SA life type in seconds
01:50:37: ISAKMP:      SA life duration (basic) of 3600
01:50:37: ISAKMP:      SA life type in kilobytes
01:50:37: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
01:50:37: ISAKMP:      authenticator is HMAC-MD5
01:50:37: validate proposal 0
01:50:37: ISAKMP (0:1): atts are acceptable.
01:50:37: ISAKMP (0:1): Checking IPSec proposal 1
01:50:37: ISAKMP: transform 1, ESP_DES
```

```
01:50:37: ISAKMP:   attributes in transform:
01:50:37: ISAKMP:      encaps is 1
01:50:37: ISAKMP:      SA life type in seconds
01:50:37: ISAKMP:      SA life duration (basic) of 3600
01:50:37: ISAKMP:      SA life type in kilobytes
01:50:37: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
01:50:37: validate proposal 0
01:50:37: ISAKMP (0:1): atts are acceptable.
01:50:37: IPSec(validate_proposal_request): proposal part #1,
  (key Eng. msg.) dest= 19.19.19.19, src= 18.18.18.18,
  dest_proxy= 19.19.1!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 30/40/70 ms
ubr904-2#
```

請注意，第一次ping失敗。這是因為需要建立連線。

uBR924-1顯示以下調試輸出：

```
ubr924-1#
01:50:24: ISAKMP (1): received packet from 18.18.18.18 (R) QM_IDLE
01:50:24: CryptoEngine0: generate hmac context for conn id 1
01:50:24: ISAKMP (0:1): processing SA payload. Message ID = 1108017901
01:50:24: ISAKMP (0:1): Checking IPSec proposal 1
01:50:24: ISAKMP: transform 1, AH_MD5
01:50:24: ISAKMP:   attributes in transform:
01:50:24: ISAKMP:      encaps is 1
01:50:24: ISAKMP:      SA life type in seconds
01:50:24: ISAKMP:      SA life duration (basic) of 3600
01:50:24: ISAKMP:      SA life type in kilobytes
01:50:24: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
01:50:24: ISAKMP:      authenticator is HMAC-MD5
01:50:24: validate proposal 0
01:50:24: ISAKMP (0:1): atts are acceptable.
01:50:24: ISAKMP (0:1): Checking IPSec proposal 1
01:50:24: ISAKMP: transform 1, ESP_DES
01:50:24: ISAKMP:   attributes in transform:
01:50:24: ISAKMP:      encaps is 1
01:50:24: ISAKMP:      SA life type in seconds
01:50:24: ISAKMP:      SA life duration (basic) of 3600
01:50:24: ISAKMP:      SA life type in kilobytes
01:50:24: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
01:50:24: validate proposal 0
01:50:24: ISAKMP (0:1): atts are acceptable.
01:50:24: IPSec(validate_proposal_request): proposal part #1,
  (key Eng. msg.) dest= 19.19.19.19, src= 18.18.18.18,
    dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4),
    src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4),
    protocol= AH, transform= ah-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
01:50:24: IPSec(validate_proposal_request): proposal part #2,
  (key Eng. msg.) dest= 19.19.19.19, src= 18.18.18.18,
    dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4),
    src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= ESP-Des ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
01:50:24: validate proposal request 0
01:50:24: ISAKMP (0:1): processing NONCE payload. Message ID = 1108017901
01:50:24: ISAKMP (0:1): processing ID payload. Message ID = 1108017901
01:50:24: ISAKMP (1): ID_IPV4_ADDR_SUBNET src 18.18.18.0/255.255.255.0
   prot 0 Port 0
```

```
01:50:24: ISAKMP (0:1): processing ID payload. Message ID = 1108017901
01:50:24: ISAKMP (1): ID_IPV4_ADDR_SUBNET dst 19.19.19.0/255.255.255.0
   prot 0 Port 0
01:50:24: ISAKMP (0:1): asking for 2 spis from IPSec
01:50:24: IPSec(key_engine): got a queue event...
01:50:24: IPSec(spi_response): getting spi 393021796 for SA
        from 18.18.18.18     to 19.19.19.19     for prot 2
01:50:24: IPSec(spi_response): getting spi 45686884 for SA
        from 18.18.18.18     to 19.19.19.19     for prot 3
01:50:24: ISAKMP: received ke message (2/2)
01:50:24: CryptoEngine0: generate hmac context for conn id 1
01:50:24: ISAKMP (1): sending packet to 18.18.18.18 (R) QM_IDLE
01:50:24: ISAKMP (1): received packet from 18.18.18.18 (R) QM_IDLE
01:50:24: CryptoEngine0: generate hmac context for conn id 1
01:50:24: IPSec allocate flow 0
01:50:24: IPSec allocate flow 0
01:50:24: ISAKMP (0:1): Creating IPSec SAs
01:50:24:         inbound SA from 18.18.18.18 to 19.19.19.19
                  (proxy 18.18.18.0 to 19.19.19.0)
01:50:24:         has spi 393021796 and conn_id 2000 and flags 4
01:50:24:         lifetime of 3600 seconds
01:50:24:         lifetime of 4608000 kilobytes
01:50:24:         outbound SA from 19.19.19.19 to 18.18.18.18
                  (proxy 19.19.19.0 to 18.18.18.0)
01:50:24:         has spi 428939798 and conn_id 2001 and flags 4
01:50:24:         lifetime of 3600 seconds
01:50:24:         lifetime of 4608000 kilobytes
01:50:24: ISAKMP (0:1): Creating IPSec SAs
01:50:24:         inbound SA from 18.18.18.18 to 19.19.19.19
                  (proxy 18.18.18.0 to 19.19.19.0)
01:50:24:         has spi 45686884 and conn_id 2002 and flags 4
01:50:24:         lifetime of 3600 seconds
01:50:24:         lifetime of 4608000 kilobytes
01:50:24:         outbound SA from 19.19.19.19 to 18.18.18.18
                  (proxy 19.19.19.0 to 18.18.18.0)
01:50:24:         has spi 118036865 and conn_id 2003 and flags 4
01:50:25:         lifetime of 3600 seconds
01:50:25:         lifetime of 4608000 kilobytes
01:50:25: ISAKMP (0:1): deleting node 1108017901 error FALSE reason
          "quick mode done (await()"
01:50:25: IPSec(key_engine): got a queue event...
01:50:25: IPSec(initialize_sas): ,
  (key Eng. msg.) dest= 19.19.19.19, src= 18.18.18.18,
    dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4),
    src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4),
    protocol= AH, transform= ah-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x176D0964(393021796), conn_id= 2000, keysize= 0, flags= 0x4
01:50:25: IPSec(initialize_sas): ,
  (key Eng. msg.) src= 19.19.19.19, dest= 18.18.18.18,
    src_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4),
    protocol= AH, transform= ah-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x19911A16(428939798), conn_id= 2001, keysize= 0, flags= 0x4
01:50:25: IPSec(initialize_sas): ,
  (key Eng. msg.) dest= 19.19.19.19, src= 18.18.18.18,
    dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4),
    src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= ESP-Des ,
    lifedur= 3600s and 4608000kb,
    spi= 0x2B92064(45686884), conn_id= 2002, keysize= 0, flags= 0x4
01:50:25: IPSec(initialize_sas): ,
  (key Eng. msg.) src= 19.19.19.19, dest= 18.18.18.18,
```

```
    src_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= ESP-Des ,
    lifedur= 3600s and 4608000kb,
    spi= 0x7091981(118036865), conn_id= 2003, keysize= 0, flags= 0x4
01:50:25: IPSec(create_sa): sa created,
  (sa) sa_dest= 19.19.19.19, sa_prot= 51,
    sa_spi= 0x176D0964(393021796),
    sa_trans= ah-md5-hmac , sa_conn_id= 2000
01:50:25: IPSec(create_sa): sa created,
  (sa) sa_dest= 18.18.18.18, sa_prot= 51,
    sa_spi= 0x19911A16(428939798),
    sa_trans= ah-md5-hmac , sa_conn_id= 2001
01:50:25: IPSec(create_sa): sa created,
  (sa) sa_dest= 19.19.19.19, sa_prot= 50,
    sa_spi= 0x2B92064(45686884),
    sa_trans= ESP-Des , sa_conn_id= 2002
01:50:25: IPSec(create_sa): sa created,
  (sa) sa_dest= 18.18.18.18, sa_prot= 50,
    sa_spi= 0x7091981(118036865),
    sa_trans= ESP-Des , sa_conn_id= 2003
ubr924-1#
```

建立IPsec通道後，可以看到連線以及加密和解密的封包。

```
ubr924-1#show crypto engine connection active
ID   Interface      IP-Address     State  Algorithm          Encrypt  Decrypt
   1                               set    HMAC_MD5+DES_56_CB       0        0
2000 cable-modem0   172.16.31.20   set    HMAC_MD5                 0       99
2001 cable-modem0   172.16.31.20   set    HMAC_MD5                99        0
2002 cable-modem0   172.16.31.20   set    DES_56_CBC               0       99
2003 cable-modem0   172.16.31.20   set    DES_56_CBC              99        0
```

第一個200x行顯示收到的99個資料包。它必須解密資料包才能將其傳送到PC1。第二行顯示已傳送的99個資料包。它必須在將資料包傳送到uBR904-2之前對其進行加密。第三和第四行執行相同的過程，但使用ESP-DES轉換而不是AH-MD5-HMAC。

註：如果在電纜數據機上配置的轉換集是ESP-DES ESP-MD5-HMAC，則您只能看到兩個自治系統(AS)，與前面的**show**命令中顯示的四個不同。

```
ubr904-2#show crypto engine connection active
ID   Interface      IP-Address     State  Algorithm          Encrypt  Decrypt
   1                               set    HMAC_MD5+DES_56_CB       0        0
2000 cable-modem0   172.16.30.18   set    HMAC_MD5                 0       99
2001 cable-modem0   172.16.30.18   set    HMAC_MD5                99        0
2002 cable-modem0   172.16.30.18   set    DES_56_CBC               0       99
2003 cable-modem0   172.16.30.18   set    DES_56_CBC              99        0
```

從uBR924-1向PC2發出擴展ping命令，檢視加密和解密資料包的計數器是否增加。

```
ubr924-1#ping ip
Target IP address: 18.18.18.1
Repeat count [5]: 50
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 19.19.19.19
Type of service [0]:
```

```
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 18.18.18.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 28/30/33 ms

ubr924-1#show crypto engine connection active
ID   Interface      IP-Address     State  Algorithm          Encrypt  Decrypt
   1                               set    HMAC_MD5+DES_56_CB       0        0
2000 cable-modem0   172.16.31.20   set    HMAC_MD5                 0      149
2001 cable-modem0   172.16.31.20   set    HMAC_MD5               149        0
2002 cable-modem0   172.16.31.20   set    DES_56_CBC               0      149
2003 cable-modem0   172.16.31.20   set    DES_56_CBC             149        0

ubr904-2#show crypto engine connection active
ID   Interface      IP-Address     State  Algorithm          Encrypt  Decrypt
   1                               set    HMAC_MD5+DES_56_CB       0        0
2000 cable-modem0   172.16.30.18   set    HMAC_MD5                 0      149
2001 cable-modem0   172.16.30.18   set    HMAC_MD5               149        0
2002 cable-modem0   172.16.30.18   set    DES_56_CBC               0      149
2003 cable-modem0   172.16.30.18   set    DES_56_CBC             149        0
```

可以發出另一個擴展ping，以檢視計數器是否再次增加。這一次，從uBR904-2向uBR924-1(19.19.19.19)的乙太網介面傳送500資料包ping。

```
ubr904-2#ping ip
Target IP address: 19.19.19.19
Repeat count [5]: 500
Datagram size [100]: 1000
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 18.18.18.18
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 500, 1000-byte ICMP Echos to 19.19.19.19, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
01:59:06: IPSec(encapsulate): encaps area too small, moving to new buffer:
idbtype 0, encaps_size 26, header size 60, avail 84!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 98/135/352 ms

ubr904-2#show crypto engine connection active
ID   Interface      IP-Address     State  Algorithm          Encrypt  Decrypt
   1                               set    HMAC_MD5+DES_56_CB       0        0
2000 cable-modem0   172.16.30.18   set    HMAC_MD5                 0      649
2001 cable-modem0   172.16.30.18   set    HMAC_MD5               649        0
```

```
2002 cable-modem0   172.16.30.18   set    DES_56_CBC               0      649
2003 cable-modem0   172.16.30.18   set    DES_56_CBC             649        0

ubr924-1#show crypto engine connection active
ID   Interface      IP-Address     State  Algorithm          Encrypt  Decrypt
   1                               set    HMAC_MD5+DES_56_CB       0        0
2000 cable-modem0   172.16.31.20   set    HMAC_MD5                 0      649
2001 cable-modem0   172.16.31.20   set    HMAC_MD5               649        0
2002 cable-modem0   172.16.31.20   set    DES_56_CBC               0      649
2003 cable-modem0   172.16.31.20   set    DES_56_CBC             649        0
```

您可以發出**clear crypto isakmp**和**clear crypto sa**命令以清除連線。此外，如果在到期時間內沒有通過IPsec隧道的流量，則IPsec會自動重置連線。

疑難排解

目前尚無特定資訊可用於排解此組態的疑難問題。

相關資訊

- IPsec網路安全命令
- IP安全(IPsec)加密簡介 — 調試資訊
- IPsec配置示例
- 配置IPsec網路安全
- 配置Cisco uBR900系列電纜接入路由器
- Cisco Cable/Broadband下載(僅限註冊客戶)
- 寬頻纜線技術支援
- 技術支援與文件 - Cisco Systems