設定IPSec通道端點探索

目錄

簡介

通道端點探索(TED)是Cisco IOS®軟體功能，允許路由器自動探索IP安全(IPsec)端點。使用網際網路金鑰交換(IKE)部署IPsec時，需要為每個對等點設定加密映像，以識別要建立安全通道的端點。當要建立隧道的對等體較多時，此方法不能很好地擴展。動態加密對映通過自動確定IPsec對等體來簡化此類場景。這僅適用於接收IKE請求的路由器。TED允許發起和接收IKE請求的路由器動態發現IPsec隧道端點。

TED使用發現探測，即從發起對等體向原始流量發往的目的網路或主機傳送的特殊IKE資料包。由於TED探測使用受保護實體的地址，因此這些地址必須可全域性路由。如果涉及網路地址轉換(NAT)，則TED不起作用。

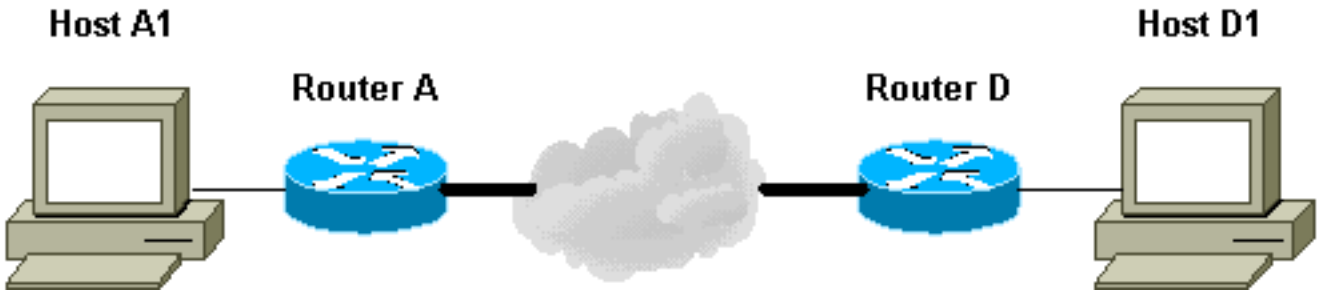
必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- IP Security(IPSec)加密簡介中討論的IPsec知識和配置

本示例網路顯示了TED過程的工作原理。



1. D1傳送一個指向A1的資料包。SRC=D1 DST=A1
2. D收到該資料包，發現它未建立IPsec安全關聯(SA)（但它確實在訪問清單的範圍內），丟棄該資料包，並傳送一個針對A1的TED探測資料包（查詢遠端對等體是誰），並在負載中嵌入IP地址D。SRC=D1DST=A1Data=IP_of_D
3. TED探測資料包到達A，後者將其識別為TED探測資料包。捨棄封包，因為D1和A1之間的任何流量都應加密。然後向D傳送一個TED應答資料包，並在負載中新增A的IP地址。這是因為D需要知道它需要使用哪個路由器來建立IPsec SA，這就是為什麼D最初將TED探測資料包傳送出去。SRC=ADST=DData=IP_of_A
4. TED應答資料包到達D。由於D現在知道IKE端點，它可以以主模式或主動模式啟動到A的隧道。

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據.

- Cisco IOS 軟體版本 12.2(27)
- Cisco 2600路由器

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。

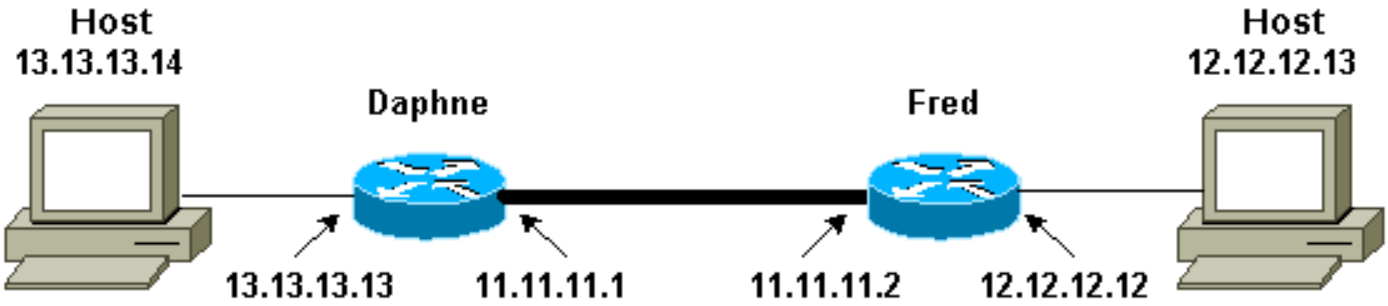
設定

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(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：



注意：在路由器Daphne和Fred之間建立隧道。

組態

本檔案會使用以下設定：

- 達芙妮
- 弗雷德

Daphne組態

```
Daphne#show running-config
Building configuration...

Current configuration : 1426 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Daphne
!
boot system flash  c2600-jk9s-mz.122-27.bin


enable password cisco
!

memory-size iomem 10
ip subnet-zero
!
!
no ip domain-lookup
!
!
!
!
!--- Defines the IKE policy. While using TED, the peer
!--- address associated with the pre-shared key should
be defined as wildcard !--- in the IKE policy, to
authenticate any discovered peer. crypto isakmp policy
10
 authentication pre-share
crypto isakmp key abc123 address 0.0.0.0 0.0.0.0
!
!
!--- Defines the transform to use for IPsec SAs. crypto
ipsec transform-set ted-transforms esp-des esp-md5-hmac
!
```

```
!--- Defines a dynamic crypto map to use for
establishing IPsec SAs. crypto dynamic-map ted-map 10
 set transform-set ted-transforms
 match address 101
!
!
!--- The 'discover' keyword used with the dynamic crypto
map !--- enables peer discovery. crypto map tedtag 10
ipsec-isakmp dynamic ted-map discover
!


!
interface FastEthernet0/0
 ip address 11.11.11.1 255.255.255.0
 duplex auto
 speed auto
 crypto map tedtag
!
interface FastEthernet0/1
 ip address 13.13.13.13 255.255.255.0
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 11.11.11.2
ip http server

!
!
!
!--- Defines the traffic to be encrypted using IPsec.
access-list 101 permit ip 13.13.13.0 0.0.0.255
12.12.12.0 0.0.0.255

!
!
!--- Output is suppressed. ! ! line con 0 line aux 0
line vty 0 4 login ! end
```

弗雷德配置

```
fred#show running-config
Building configuration...

Current configuration : 1295 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname fred
!
boot system flash  c2600-jk9s-mz.122-27.bin


!
memory-size iomem 10
ip subnet-zero
!
!
!
```

```
!
!
!
!--- Defines the IKE policy. While using TED, the peer
!--- address associated with the pre-shared key should
be defined as wildcard !--- in the IKE policy, to
authenticate any discovered peer. crypto isakmp policy
10
 authentication pre-share
crypto isakmp key abc123 address 0.0.0.0 0.0.0.0
!
!
!--- Defines the transform to use for IPsec SAs. crypto
ipsec transform-set ted-transforms esp-des esp-md5-hmac
!
!--- Defines a dynamic crypto map used to establish
IPsec SAs. crypto dynamic-map ted-map 10
 set transform-set ted-transforms
 match address 101
!
!
!--- The 'discover' keyword used with the dynamic crypto
map !--- enables peer discovery. crypto map tedtag 10
ipsec-isakmp dynamic ted-map discover
!

!
!
interface FastEthernet0/0
 ip address 11.11.11.2 255.255.255.0
 duplex auto
 speed auto
 crypto map tedtag
!
interface FastEthernet0/1
 ip address 12.12.12.12 255.255.255.0
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 11.11.11.1
ip http server

!
!
!
!--- Defines the traffic encrypted using IPsec. access-
list 101 permit ip 12.12.12.0 0.0.0.255 13.13.13.0
0.0.0.255

!
!
!--- Output is suppressed. ! line con 0 line aux 0 line
vty 0 4 login ! end
```

驗證

使用本節內容，確認您的組態是否正常運作。

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。

- show crypto isakmp sa — 通過顯示路由器的IKE SA顯示第1階段的安全關聯。所顯示的狀態是QM_IDLE，IKE SA將被視為已啟動並正常運行。
- show crypto ipsec sa — 顯示路由器活動IPsec SA的詳細清單，顯示第2階段的安全關聯。
- show crypto map — 顯示路由器上配置的加密對映及其詳細資訊，如加密訪問清單、轉換集、對等體等。
- show crypto engine connections active — 顯示活動SA及其關聯介面、轉換和計數器的清單。

顯示輸出示例

本節擷取路由器Daphne上的**show**命令輸出(當在主機13.13.13.4上執行針對主機12.12.13的**ping**命令時)。路由器Fred上的輸出也是類似的。輸出中的關鍵引數以粗體顯示。如需命令輸出的說明，請參閱IP安全性疑難排解 — 瞭解和使用debug命令。

```
Daphne#show crypto isakmp sa
dst             src             state          conn-id    slot
11.11.11.2      11.11.11.1      QM_IDLE              2       0


Daphne#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: tedtag, local addr. 11.11.11.1

   protected vrf:
   local  ident (addr/mask/prot/port): (13.13.13.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (12.12.12.0/255.255.255.0/0/0)
   current_peer: 11.11.11.2
     PERMIT, flags={}
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest 9
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify 9
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 11.11.11.1, remote crypto endpt.: 11.11.11.2
     path mtu 1500, media mtu 1500
     current outbound spi: B326CBE6

     inbound esp sas:
      spi: 0xD8870500(3632727296)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: tedtag
        sa timing: remaining key lifetime (k/sec): (4414715/2524)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB326CBE6(3005664230)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: tedtag
        sa timing: remaining key lifetime (k/sec): (4414715/2524)
```

```
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:


Daphne#show crypto map
Crypto Map "tedtag" 10 ipsec-isakmp
        Dynamic map template tag: ted-map
        Discover enabled

Crypto Map "tedtag" 11 ipsec-isakmp
        Peer = 11.11.11.2
        Extended IP access list
            access-list  permit ip 13.13.13.0 0.0.0.255 12.12.12.0 0.0.0.255
            dynamic (created from dynamic map ted-map/10)
        Current peer: 11.11.11.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={ ted-transforms, }
        Interfaces using crypto map tedtag:
                FastEthernet0/0


Daphne#show crypto engine connections active
  ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
   2 <none>               <none>          set    HMAC_SHA+DES_56_CB        0        0
2000 FastEthernet0/0      11.11.11.1      set    HMAC_MD5+DES_56_CB        0        9
2001 FastEthernet0/0      11.11.11.1      set    HMAC_MD5+DES_56_CB        9        0
```

疑難排解

使用本節內容，對組態進行疑難排解。

疑難排解指令

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

- debug crypto engine — 顯示有關執行加密和解密過程的加密引擎的資訊。
- debug crypto ipsec — 顯示第2階段的IPsec協商。
- debug crypto isakmp — 顯示第1階段的IKE協商。

調試輸出示例

本節擷取在主機13.13.13.4上執行ping指令時（目的地為主機12.12.13）在設定了IPsec的路由器上所輸出的debug指令。

- 達芙妮
- 弗雷德

達芙妮

```
Daphne#show debug
```

```
Cryptographic Subsystem:
  Crypto ISAKMP debugging is on
  Crypto Engine debugging is on
  Crypto IPSEC debugging is on
Daphne#
!--- TED process begins here. *Mar  1 02:07:18.850: IPSEC(tunnel discover request): ,
  (key eng. msg.) INBOUND local= 13.13.13.14, remote= 12.12.12.13,
    local_proxy= 13.13.13.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 11.11.11.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004 dest=FastEthernet0
    /0:11.11.11.2
*Mar  1 02:07:18.854: ISAKMP: received ke message (1/1)
*Mar  1 02:07:18.854: ISAKMP: GOT A PEER DISCOVERY MESSAGE FROM THE SA MANAGER!!!
*Mar  1 02:07:18.854: src = 13.13.13.14 to 12.12.12.13, protocol 3,
   transform 2, hmac 1
*Mar  1 02:07:18.854: proxy source is 13.13.13.0/255.255.255.0 and my
   address (not used now) is 11.11.11.1
!--- IKE uses UDP port 500. *Mar 1 02:07:18.854: ISAKMP: local port 500, remote port 500

*Mar  1 02:07:18.858: ISAKMP (0:1): no idb in request
*Mar  1 02:07:18.858: ISAKMP (1): ID payload
        next-payload : 5
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
*Mar  1 02:07:18.858: ISAKMP (1): Total payload length: 12
*Mar  1 02:07:18.858: 1st ID is 11.11.11.1
*Mar  1 02:07:18.862: 2nd ID is 13.13.13.0/255.255.255.0
*Mar  1 02:07:18.862: ISAKMP (0:1): beginning peer discovery exchange
!--- TED probe is sent to the original destination of the !--- IP packet that matches the crypto
access-list for encryption. *Mar  1 02:07:18.862: ISAKMP (0:1): sending packet to 12.12.12.13
(I)
PEER_DISCOVERY via FastEthernet0/0:11.11.11.2
!--- TED response is received and the peer discovered. *Mar  1 02:07:18.962: ISAKMP (0:1):
received packet from
11.11.11.2 (I) PEER_DISCOVERY
*Mar  1 02:07:18.966: ISAKMP (0:1): processing vendor id payload
*Mar  1 02:07:18.966: ISAKMP (0:1): speaking to another IOS box!
*Mar  1 02:07:18.966: ISAKMP (0:1): processing ID payload. message ID = 0
*Mar  1 02:07:18.966: ISAKMP:received payload type 16
*Mar  1 02:07:18.966: ISAKMP (0:1): received response to my peer discovery probe!
*Mar  1 02:07:18.966: ISAKMP (0:1): ted negotiated proxies:
 0 13.13.13.0/255.255.255.0:0, 12.12.12.0
/255.255.255.0:0
!--- Normal IKE process begins here to form a secure tunnel to the !--- peer discovered through
TED. *Mar  1 02:07:18.970: ISAKMP (0:1): initiating IKE to 11.11.11.2
 in response to probe.
*Mar  1 02:07:18.970: ISAKMP: local port 500, remote port 500
*Mar  1 02:07:18.970: ISAKMP (0:1): created new SA after peer-discovery
  with 11.11.11.2
*Mar  1 02:07:18.974: ISAKMP (0:2): sending packet to 11.11.11.2 (I) MM_NO_STATE
*Mar  1 02:07:18.974: ISAKMP (0:1): peer does not do paranoid keepalives.

*Mar  1 02:07:18.974: ISAKMP (0:1): deleting SA reason "delete_me flag/throw"
state (I) PEER_DISCOVE
RY (peer 12.12.12.13) input queue 0
*Mar  1 02:07:19.975: ISAKMP (0:1): purging SA., sa=82687F70, delme=82687F70
*Mar  1 02:07:19.975: CryptoEngine0: delete connection 1
*Mar  1 02:07:20.608: ISAKMP (0:2): received packet from 11.11.11.2 (I) MM_NO_STATE
*Mar  1 02:07:20.608: ISAKMP (0:2): processing SA payload. message ID = 0
*Mar  1 02:07:20.608: ISAKMP (0:2): found peer pre-shared key matching 11.11.11.2
```

```
!--- IKE SAs are negotiated. *Mar  1 02:07:20.612: ISAKMP (0:2): Checking ISAKMP transform 1
against priority 10 policy
*Mar  1 02:07:20.612: ISAKMP:      encryption DES-CBC
*Mar  1 02:07:20.612: ISAKMP:      hash SHA
*Mar  1 02:07:20.612: ISAKMP:      default group 1
*Mar  1 02:07:20.612: ISAKMP:      auth pre-share
*Mar  1 02:07:20.612: ISAKMP:      life type in seconds
*Mar  1 02:07:20.612: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Mar  1 02:07:20.612: ISAKMP (0:2): atts are acceptable. Next payload is 0
*Mar  1 02:07:20.616: CryptoEngine0: generate alg parameter
*Mar  1 02:07:20.781: CRYPTO_ENGINE: Dh phase 1 status: 0
*Mar  1 02:07:20.781: CRYPTO_ENGINE: Dh phase 1 status: 0
*Mar  1 02:07:20.781: ISAKMP (0:2): SA is doing pre-shared key authentication
      using id type ID_IPV4_ADDR
*Mar  1 02:07:20.797: ISAKMP (0:2): sending packet to 11.11.11.2 (I) MM_SA_SETUP
*Mar  1 02:07:22.972: ISAKMP (0:2): received packet from 11.11.11.2 (I) MM_SA_SETUP
*Mar  1 02:07:22.972: ISAKMP (0:2): processing KE payload. message ID = 0
*Mar  1 02:07:22.972: CryptoEngine0: generate alg parameter
*Mar  1 02:07:23.177: ISAKMP (0:2): processing NONCE payload. message ID = 0
*Mar  1 02:07:23.177: ISAKMP (0:2): found peer pre-shared key matching 11.11.11.2
*Mar  1 02:07:23.181: CryptoEngine0: create ISAKMP SKEYID for conn id 2
*Mar  1 02:07:23.181: ISAKMP (0:2): SKEYID state generated
*Mar  1 02:07:23.185: ISAKMP (0:2): processing vendor id payload
*Mar  1 02:07:23.185: ISAKMP (0:2): speaking to another IOS box!
*Mar  1 02:07:23.185: ISAKMP (2): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
*Mar  1 02:07:23.185: ISAKMP (2): Total payload length: 12
*Mar  1 02:07:23.185: CryptoEngine0: generate hmac context for conn id 2
*Mar  1 02:07:23.189: ISAKMP (0:2): sending packet to 11.11.11.2 (I) MM_KEY_EXCH
*Mar  1 02:07:23.277: ISAKMP (0:2): received packet from 11.11.11.2 (I) MM_KEY_EXCH
*Mar  1 02:07:23.281: ISAKMP (0:2): processing ID payload. message ID = 0
*Mar  1 02:07:23.281: ISAKMP (0:2): processing HASH payload. message ID = 0
*Mar  1 02:07:23.281: CryptoEngine0: generate hmac context for conn id 2
!--- Peer is authenticated. *Mar  1 02:07:23.285: ISAKMP (0:2): SA has been authenticated with
11.11.11.2
*Mar  1 02:07:23.285: ISAKMP (0:2): beginning Quick Mode exchange, M-ID of 409419560
*Mar  1 02:07:23.285: ISAKMP (0:2): asking for 1 spis from ipsec
*Mar  1 02:07:23.285: ISAKMP (0:2): had to get SPI's from ipsec.
*Mar  1 02:07:23.289: CryptoEngine0: clear dh number for conn id 1
*Mar  1 02:07:23.289: IPSEC(key_engine): got a queue event...
*Mar  1 02:07:23.289: IPSEC(spi_response): getting spi 4160804383 for SA
        from 11.11.11.1      to 11.11.11.2      for prot 3
*Mar  1 02:07:23.289: ISAKMP: received ke message (2/1)
*Mar  1 02:07:23.537: CryptoEngine0: generate hmac context for conn id 2
*Mar  1 02:07:23.541: ISAKMP (0:2): sending packet to 11.11.11.2 (I) QM_IDLE
*Mar  1 02:07:23.958: ISAKMP (0:2): received packet from 11.11.11.2 (I) QM_IDLE
*Mar  1 02:07:23.962: CryptoEngine0: generate hmac context for conn id 2
*Mar  1 02:07:23.962: ISAKMP (0:2): processing HASH payload. message ID = 409419560
*Mar  1 02:07:23.962: ISAKMP (0:2): processing SA payload. message ID = 409419560
!--- IPsec SAs are negotiated. *Mar  1 02:07:23.962: ISAKMP (0:2): Checking IPSec proposal 1
*Mar  1 02:07:23.962: ISAKMP: transform 1, ESP_DES
*Mar  1 02:07:23.966: ISAKMP:   attributes in transform:
*Mar  1 02:07:23.966: ISAKMP:      encaps is 1
*Mar  1 02:07:23.966: ISAKMP:      SA life type in seconds
*Mar  1 02:07:23.966: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 02:07:23.966: ISAKMP:      SA life type in kilobytes
*Mar  1 02:07:23.966: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Mar  1 02:07:23.966: ISAKMP:      authenticator is HMAC-MD5
*Mar  1 02:07:23.970: validate proposal 0
*Mar  1 02:07:23.970: ISAKMP (0:2): atts are acceptable.
```

```
*Mar  1 02:07:23.970: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 11.11.11.1, remote= 11.11.11.2,
    local_proxy= 13.13.13.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 12.12.12.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 02:07:23.974: validate proposal request 0
*Mar  1 02:07:23.974: ISAKMP (0:2): processing NONCE payload. message ID = 409419560
*Mar  1 02:07:23.974: ISAKMP (0:2): processing ID payload. message ID = 409419560
*Mar  1 02:07:23.974: ISAKMP (0:2): processing ID payload. message ID = 409419560
*Mar  1 02:07:23.974: CryptoEngine0: generate hmac context for conn id 2
*Mar  1 02:07:23.978: ipsec allocate flow 0
*Mar  1 02:07:23.978: ipsec allocate flow 0
!--- IPsec SAs are generated for inbound and outbound traffic. *Mar  1 02:07:23.986: ISAKMP
(0:2): Creating IPSec SAs
*Mar  1 02:07:23.986:         inbound SA from 11.11.11.2 to 11.11.11.1
        (proxy 12.12.12.0 to 13.13.13.0)
*Mar  1 02:07:23.986:         has spi 0xF800D61F and conn_id 2000 and flags 4
*Mar  1 02:07:23.986:         lifetime of 3600 seconds
*Mar  1 02:07:23.986:         lifetime of 4608000 kilobytes
*Mar  1 02:07:23.990: outbound SA from 11.11.11.1 to 11.11.11.2
(proxy 13.13.13.0 to 12.12.12.0     )
*Mar  1 02:07:23.990: has spi -1535570016 and conn_id 2001 and flags C
*Mar  1 02:07:23.990:         lifetime of 3600 seconds
*Mar  1 02:07:23.990:         lifetime of 4608000 kilobytes
*Mar  1 02:07:23.990: ISAKMP (0:2): sending packet to 11.11.11.2 (I) QM_IDLE
*Mar  1 02:07:23.994: ISAKMP (0:2): deleting node 409419560 error FALSE reason ""
*Mar  1 02:07:23.994: IPSEC(key_engine): got a queue event...
*Mar  1 02:07:23.994: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 11.11.11.1, remote= 11.11.11.2,
    local_proxy= 13.13.13.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 12.12.12.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xF800D61F(4160804383), conn_id= 2000, keysize= 0, flags= 0x4
*Mar  1 02:07:23.998: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 11.11.11.1, remote= 11.11.11.2,
    local_proxy= 13.13.13.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 12.12.12.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA4790FA0(2759397280), conn_id= 2001, keysize= 0, flags= 0xC
*Mar  1 02:07:24.002: IPSEC(create_sa): sa created,
  (sa) sa_dest= 11.11.11.1, sa_prot= 50,
    sa_spi= 0xF800D61F(4160804383),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
*Mar  1 02:07:24.002: IPSEC(create_sa): sa created,
  (sa) sa_dest= 11.11.11.2, sa_prot= 50,
    sa_spi= 0xA4790FA0(2759397280),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001


Daphne#
```

弗雷德

```
fred#show debug

Cryptographic Subsystem:
  Crypto ISAKMP debugging is on
  Crypto Engine debugging is on
  Crypto IPSEC debugging is on
```

```
fred#
!--- Receives the TED probe. *Mar  1 02:07:45.763: ISAKMP (0:0): received packet from
 13.13.13.14 (N) NEW SA
*Mar  1 02:07:45.767: ISAKMP: local port 500, remote port 500
*Mar  1 02:07:45.779: ISAKMP (0:1): processing vendor id payload
*Mar  1 02:07:45.783: ISAKMP (0:1): speaking to another IOS box!
*Mar  1 02:07:45.783: ISAKMP (0:1): processing ID payload. message ID = 0
*Mar  1 02:07:45.787: ISAKMP (0:1): processing ID payload. message ID =
 -1992472852
*Mar  1 02:07:45.791: ISAKMP (1): ID_IPV4_ADDR_SUBNET src 13.13.13.0
 /255.255.255.0 prot 0 port 0
*Mar  1 02:07:45.791: ISAKMP (0:1): processing vendor id payload
!--- Sends a response to the other peer for the TED probe. *Mar  1 02:07:45.795: ISAKMP (0:1):
responding to peer discovery probe!
*Mar  1 02:07:45.799: peer's address is 11.11.11.1
*Mar  1 02:07:45.799: src (him) 4, 13.13.13.0/255.255.255.0 to dst
(me) 0, 0.0.0.0/0.0.0.0
*Mar  1 02:07:45.803: ISAKMP (0:1): peer can handle TED V3: changing source
to 11.11.11.1 and dest to 11.11.11.2
*Mar  1 02:07:45.811: ISAKMP (1): ID payload
        next-payload : 239
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
*Mar  1 02:07:45.815: ISAKMP (1): Total payload length: 12
*Mar  1 02:07:45.819: ISAKMP (0:1): sending packet to 11.11.11.1 (R)
 PEER_DISCOVERY
*Mar  1 02:07:45.823: ISAKMP (0:1): peer does not do paranoid keepalives.

*Mar  1 02:07:45.823: ISAKMP (0:1): deleting SA reason "delete_me flag/throw"
state (R) PEER_DISCOVE
RY (peer 11.11.11.1) input queue 0
*Mar  1 02:07:45.827: ISAKMP (0:1): deleting node 0 error TRUE reason
"delete_me flag/throw"
 !--- IKE processing begins here. *Mar  1 02:07:45.871: ISAKMP (0:0): received packet from
11.11.11.1
(N) NEW SA
*Mar  1 02:07:45.875: ISAKMP: local port 500, remote port 500
*Mar  1 02:07:45.883: ISAKMP (0:2): processing SA payload. message ID = 0
*Mar  1 02:07:45.887: ISAKMP (0:2): found peer pre-shared key matching 11.11.11.1
!--- IKE SAs are negotiated. *Mar  1 02:07:45.887: ISAKMP (0:2): Checking ISAKMP transform 1
against priority 10 policy
*Mar  1 02:07:45.891: ISAKMP:      encryption DES-CBC
*Mar  1 02:07:45.891: ISAKMP:      hash SHA
*Mar  1 02:07:45.895: ISAKMP:      default group 1
*Mar  1 02:07:45.895: ISAKMP:      auth pre-share
*Mar  1 02:07:45.899: ISAKMP:      life type in seconds
*Mar  1 02:07:45.899: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Mar  1 02:07:45.903: ISAKMP (0:2): atts are acceptable. Next payload is 0
*Mar  1 02:07:45.907: CryptoEngine0: generate alg parameter
*Mar  1 02:07:47.455: CRYPTO_ENGINE: Dh phase 1 status: 0
*Mar  1 02:07:47.455: CRYPTO_ENGINE: Dh phase 1 status: 0
*Mar  1 02:07:47.459: ISAKMP (0:2): SA is doing pre-shared key authentication
using id type ID_IPV4_
ADDR
*Mar  1 02:07:47.463: ISAKMP (0:2): sending packet to 11.11.11.1 (R) MM_SA_SETUP
*Mar  1 02:07:47.467: ISAKMP (0:1): purging SA., sa=2349E0, delme=2349E0
*Mar  1 02:07:47.471: ISAKMP (0:1): purging node 0
*Mar  1 02:07:47.475: CryptoEngine0: delete connection 1
*Mar  1 02:07:47.707: ISAKMP (0:2): received packet from 11.11.11.1 (R) MM_SA_SETUP
*Mar  1 02:07:47.711: ISAKMP (0:2): processing KE payload. message ID = 0
*Mar  1 02:07:47.715: CryptoEngine0: generate alg parameter
*Mar  1 02:07:49.767: ISAKMP (0:2): processing NONCE payload. message ID = 0
```

```
*Mar  1 02:07:49.775: ISAKMP (0:2): found peer pre-shared key matching 11.11.11.1
*Mar  1 02:07:49.783: CryptoEngine0: create ISAKMP SKEYID for conn id 2
*Mar  1 02:07:49.799: ISAKMP (0:2): SKEYID state generated
*Mar  1 02:07:49.803: ISAKMP (0:2): processing vendor id payload
*Mar  1 02:07:49.807: ISAKMP (0:2): speaking to another IOS box!
*Mar  1 02:07:49.815: ISAKMP (0:2): sending packet to 11.11.11.1 (R) MM_KEY_EXCH
*Mar  1 02:07:50.087: ISAKMP (0:2): received packet from 11.11.11.1 (R) MM_KEY_EXCH
*Mar  1 02:07:50.095: ISAKMP (0:2): processing ID payload. message ID = 0
*Mar  1 02:07:50.099: ISAKMP (0:2): processing HASH payload. message ID = 0
*Mar  1 02:07:50.103: CryptoEngine0: generate hmac context for conn id 2
!--- Peer is authenticated. *Mar  1 02:07:50.111: ISAKMP (0:2): SA has been authenticated with
11.11.11.1
*Mar  1 02:07:50.115: ISAKMP (2): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
*Mar  1 02:07:50.115: ISAKMP (2): Total payload length: 12
*Mar  1 02:07:50.119: CryptoEngine0: generate hmac context for conn id 2
*Mar  1 02:07:50.131: CryptoEngine0: clear dh number for conn id 1
*Mar  1 02:07:50.135: ISAKMP (0:2): sending packet to 11.11.11.1 (R) QM_IDLE
*Mar  1 02:07:50.451: ISAKMP (0:2): received packet from 11.11.11.1 (R) QM_IDLE
*Mar  1 02:07:50.467: CryptoEngine0: generate hmac context for conn id 2
*Mar  1 02:07:50.475: ISAKMP (0:2): processing HASH payload. message ID = 409419560
*Mar  1 02:07:50.475: ISAKMP (0:2): processing SA payload. message ID = 409419560
!--- IPsec SAs are negotiated. *Mar  1 02:07:50.479: ISAKMP (0:2): Checking IPSec proposal 1
*Mar  1 02:07:50.479: ISAKMP: transform 1, ESP_DES
*Mar  1 02:07:50.483: ISAKMP:   attributes in transform:
*Mar  1 02:07:50.483: ISAKMP:      encaps is 1
*Mar  1 02:07:50.487: ISAKMP:      SA life type in seconds
*Mar  1 02:07:50.487: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 02:07:50.487: ISAKMP:      SA life type in kilobytes
*Mar  1 02:07:50.491: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Mar  1 02:07:50.495: ISAKMP:      authenticator is HMAC-MD5
*Mar  1 02:07:50.495: validate proposal 0
*Mar  1 02:07:50.499: ISAKMP (0:2): atts are acceptable.
*Mar  1 02:07:50.503: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 11.11.11.2, remote= 11.11.11.1,
    local_proxy= 12.12.12.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 13.13.13.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 02:07:50.515: validate proposal request 0
*Mar  1 02:07:50.519: ISAKMP (0:2): processing NONCE payload. message
ID = 409419560
*Mar  1 02:07:50.523: ISAKMP (0:2): processing ID payload. message ID = 409419560
*Mar  1 02:07:50.523: ISAKMP (0:2): processing ID payload. message ID = 409419560
*Mar  1 02:07:50.527: ISAKMP (0:2): asking for 1 spis from ipsec
*Mar  1 02:07:50.535: IPSEC(key_engine): got a queue event...
*Mar  1 02:07:50.543: IPSEC(spi_response): getting spi 2759397280 for SA
        from 11.11.11.2      to 11.11.11.1      for prot 3
*Mar  1 02:07:50.551: ISAKMP: received ke message (2/1)
*Mar  1 02:07:50.787: CryptoEngine0: generate hmac context for conn id 2
*Mar  1 02:07:50.803: ISAKMP (0:2): sending packet to 11.11.11.1 (R) QM_IDLE
*Mar  1 02:07:50.887: ISAKMP (0:2): received packet from 11.11.11.1 (R) QM_IDLE
*Mar  1 02:07:50.899: CryptoEngine0: generate hmac context for conn id 2
*Mar  1 02:07:50.907: ipsec allocate flow 0
*Mar  1 02:07:50.907: ipsec allocate flow 0
!--- IPsec SAs are generated for inbound and outbound traffic. *Mar  1 02:07:50.939: ISAKMP
(0:2): Creating IPSec SAs
*Mar  1 02:07:50.939:         inbound SA from 11.11.11.1 to 11.11.11.2
        (proxy 13.13.13.0 to 12.12.12.0)
```

```
*Mar  1 02:07:50.947:         has spi 0xA4790FA0 and conn_id 2000 and
flags 4
*Mar  1 02:07:50.947:         lifetime of 3600 seconds
*Mar  1 02:07:50.951:         lifetime of 4608000 kilobytes
*Mar  1 02:07:50.951: outbound SA from 11.11.11.2 to 11.11.11.1
(proxy 12.12.12.0 to 13.13.13.0     )
*Mar  1 02:07:50.959:  has spi -134162913 and conn_id 2001 and flags C
*Mar  1 02:07:50.959:         lifetime of 3600 seconds
*Mar  1 02:07:50.963:         lifetime of 4608000 kilobytes
*Mar  1 02:07:50.963: ISAKMP (0:2): deleting node 409419560 error FALSE
 reason "quick mode done (awa
it()"
*Mar  1 02:07:50.971: IPSEC(key_engine): got a queue event...
*Mar  1 02:07:50.971: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 11.11.11.2, remote= 11.11.11.1,
    local_proxy= 12.12.12.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 13.13.13.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA4790FA0(2759397280), conn_id= 2000, keysize= 0, flags= 0x4
*Mar  1 02:07:50.983: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 11.11.11.2, remote= 11.11.11.1,
    local_proxy= 12.12.12.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 13.13.13.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xF800D61F(4160804383), conn_id= 2001, keysize= 0, flags= 0xC
*Mar  1 02:07:51.003: IPSEC(create_sa): sa created,
  (sa) sa_dest= 11.11.11.2, sa_prot= 50,
    sa_spi= 0xA4790FA0(2759397280),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
*Mar  1 02:07:51.007: IPSEC(create_sa): sa created,
  (sa) sa_dest= 11.11.11.1, sa_prot= 50,
    sa_spi= 0xF800D61F(4160804383),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001

fred#
```

相關資訊

- 部署IPsec
- 通道端點探索增強功能
- 技術支援與文件 - Cisco Systems