

IPSec トンネル エンドポイント ディスカバリの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[show のサンプル出力](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[debug 出力例](#)

[関連情報](#)

概要

トンネル エンドポイント ディスカバリ (TED) は、Cisco IOS® ソフトウェアの機能で、ルータで IP セキュリティ (IPSec) のエンドポイントを自動的に検出できるようにするものです。インターネット キー交換 (IKE) を使用して IPSec を導入するには、すべてのピアについて、セキュアトンネルが確立されるエンドポイントを識別するクリプト マップの設定が必要です。この方法では、多数のピアに対してトンネルが確立される場合は拡張性が低くなります。ダイナミック クリプト マップは自動的に IPSec ピアを決定することにより、このようなシナリオを簡素化します。これは IKE 要求を受信するルータでのみ機能します。TED により、IKE 要求を開始し、受信するルータは動的に IPSec トンネル エンドポイントを検出できます。

TED では、発信元ピアから宛先ネットワークまたは元のトラフィックの宛先であるホストに向けた特別な IKE パケットであるディスカバリ プローブを使用します。TED のプローブでは保護されたエンティティのアドレスを使用するため、アドレスはグローバルにルーティングする必要があります。TED は、ネットワーク アドレス変換 (NAT) が含まれる場合は機能しません。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- 『[IP Security \(IPSec\) 暗号化の概要](#)』で説明されている IPSec に関する知識と設定
このネットワークの例では、TED プロセスの動作の仕組みを示します。



1. D1はA1を対象とするデータパケットを送信します。SRC=D1 DST=A1
2. Dがこれを受信し、IPSec セキュリティ アソシエーション (SA) が確立されていないことが判明します (ただし、パケットはアクセス リストの範囲内にあります)。このパケットをドロップし、TED プロブ パケットを A1 に向けて送信します (リモートピアを識別するため)。このとき、D の IP アドレスはペイロードに組み込まれています。
SRC=D1DST=A1Data=IP_of_D
3. TED プロブ パケットが A に到達し、これが TED プロブ パケットであることが識別されます。D1 と A1 間のすべてのトラフィックは暗号化される必要があるため、このパケットはドロップされます。次に、ペイロードに A の IP アドレスを入れて、D 宛てに TED 応答パケットが送信されます。これは、IPsec SA を確立する必要があるルータを D で判明する必要があるためです。したがって、D では最初に TED プロブ パケットを送信しました。
SRC=ADST=DDData=IP_of_A
4. TED 応答パケットが D に到着します。D は IKE エンドポイントを認識しているため、メインモードまたはアグレッシブモードで A へのトンネルを開始できます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS(R) ソフトウェア リリース 12.2(27)
- Cisco 2600 ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

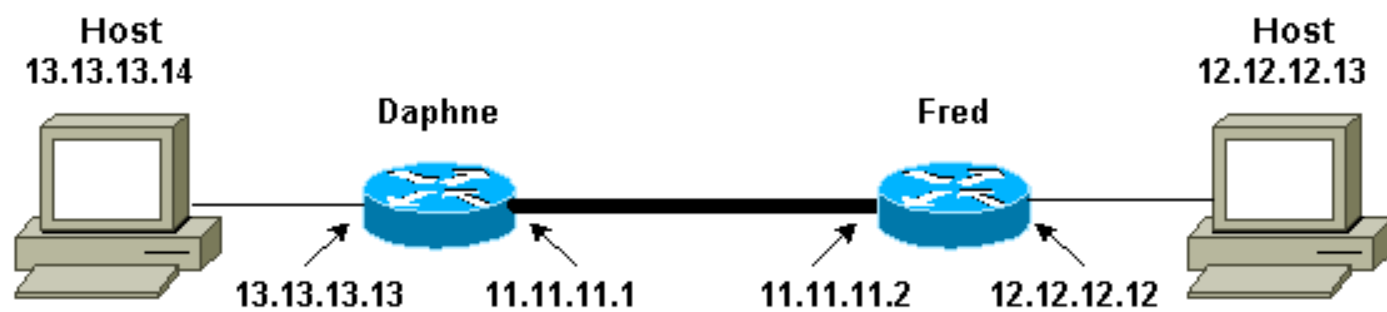
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



注：ルータDaphneとFredの間にトンネルを確立します。

設定

このドキュメントでは、次の構成を使用します。

- [Daphne](#)
- [Fred](#)

Daphne の設定

```
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
```

Fred の設定

```
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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- [show crypto isakmp sa](#) : ルータの IKE SA を表示することにより、フェーズ 1 のセキュリティ アソシエーションを表示します。表示される状態が QM_IDLE の場合、IKE SA は稼働していると見なされます。
- [show crypto ipsec sa](#) : ルータのアクティブ IPsec SA のリストを表示することにより、フェーズ 2 のセキュリティ アソシエーションを表示します。
- [show crypto map](#) : 暗号アクセス リスト、トランスフォーム セット、ピアなどの詳細を含めて、ルータに設定されている暗号マップを表示します。
- [show crypto engine connections active](#) : 関連付けられているインターフェイス、トランスフォーム、およびカウンタを含む、アクティブ SA のリストを表示します。

[show のサンプル出力](#)

このセクションでは、ホスト 13.13.13.4 でホスト 12.12.12.13 宛てに ping コマンドを実行した場合の、ルータ Daphne での show コマンドの出力をキャプチャします。ルータ Fred での出力も同様です。出力の主なパラメータは太字で示してあります。コマンド出力の説明については『[IP セキュリティのトラブルシューティング : debug コマンドの説明と使用](#)』を参照してください。

```
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

[トラブルシューティング](#)

このセクションは、設定のトラブルシューティングを行う際に参照してください。

[トラブルシューティングのためのコマンド](#)

注：[debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- [debug crypto engine](#)：暗号化と復号化プロセスを実行する暗号化エンジンに関する情報を表示します。
- [debug crypto ipsec](#)：フェーズ 2 の IPsec ネゴシエーションを表示します。
- [debug crypto isakmp](#)：フェーズ 1 の IKE ネゴシエーションを表示します。

[debug 出力例](#)

このセクションでは、IPsec が設定されているルータの debug コマンドの出力をキャプチャします。ホスト 13.13.13.4 でホスト 12.12.12.13宛てに ping コマンドを実行したときの出力です。

- [Daphne](#)
- [Fred](#)

[Daphne](#)

```
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_DISCOVER
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#

[Fred](#)

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_DISCOVER

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#

[関連情報](#)

- [IPsec の導入](#)
- [Tunnel Endpoint Discovery の拡張](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)