

Configurando o Tunnel End-Point Discovery de IPSec

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Exemplo de saída de show](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Exemplo de debug](#)

[Informações Relacionadas](#)

Introdução

O Tunnel End-Point Discovery (TED) é uma característica do software Cisco IOS® que permite que os roteadores descubram automaticamente os pontos finais da Segurança IP (IPsec). A implementação do IPsec com Internet Key Exchange (IKE) exige a configuração de um mapa de criptografia para cada par, que identifica o ponto final ao qual um túnel seguro deve ser estabelecido. Esta abordagem não é bem dimensionada quando há muitos pares a que os túneis devem ser estabelecidos. Os mapas de criptografia dinâmicos simplificam essa situação determinando automaticamente o par IPsec. Só funciona em roteadores que recebem solicitações IKE. O TED permite que os roteadores que iniciam e recebem solicitações IKE descubram dinamicamente o ponto final do túnel IPsec.

O TED usa uma prova de descoberta que seja um pacote IKE especial enviado do par de início para a rede de destino ou o host que o tráfego original esteve destinado a. Desde que as pontas de prova TED usam os endereços das entidades protegidas, os endereços devem ser globalmente roteável. O TED não trabalha se o Network Address Translation (NAT) é envolvido.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento e configuração do IPsec como discutido em uma [introdução à criptografia do protocolo de segurança IP \(IPSEC\)](#)

Esta rede de exemplo mostra como os trabalhos TED.



1. D1 envia um pacote de dados destinado a A1. SRC=D1 DST=A1
2. D recebe-o, considera que não tem uma associação de segurança IPsec (SA) estabelecida (mas cai dentro da escala da lista de acessos), deixa cair o pacote, e envia um pacote de ponta de prova TED (para encontrar quem o peer remoto seja) visado no A1, com o endereço IP de Um ou Mais Servidores Cisco ICM NT de D encaixado no payload. SRC=D1 DST=A1 Data=IP_of_D
3. O pacote de prova TED chega em A, que o reconhece como um pacote de prova TED. Deixa cair o pacote porque todo o tráfego entre o D1 e o A1 deve ser cifrado. Envia então um pacote de resposta TED visado em D com o endereço IP de Um ou Mais Servidores Cisco ICM NT de A no payload. Isto é porque D precisa de saber com que roteador precisa de estabelecer IPsec SA, que é porque D enviou inicialmente o pacote de ponta de prova TED para fora. SRC=A DST=D Data=IP_de_A
4. O pacote de resposta TED chega no D. Desde que D conhece agora o ponto final IKE, pode iniciar o túnel a A no modo principal ou no modo assertivo.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware.

- Cisco IOS Software Release 12.2(27)
- Cisco 2600 Router

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

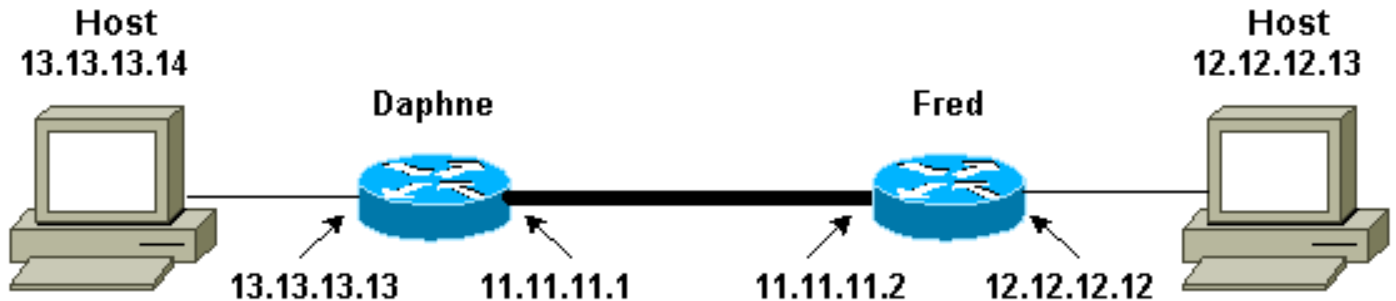
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

[Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede:



Nota: Estabeleça o túnel entre roteadores daphne e Fred.

[Configurações](#)

Este documento utiliza as seguintes configurações:

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

Configuração Daphne

```
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
```

Configuração Fred

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- [mostre isakmp crypto sa](#) — Indica as associações de segurança da fase 1 indicando IKE SA do roteador. O estado indicado é QM_IDLE para IKE SA a ser considerado acima e funcionamento.
- [mostre IPsec crypto sa](#) — Indica as associações de segurança da fase 2 indicando uma lista detalhada do IPsec ativo SA do roteador.
- [crypto map da mostra](#) — Indica os crypto map configurados no roteador junto com seus detalhes tais como Listas de acesso criptos, transformam grupos, pares, e assim por diante.
- [active do show crypto engine connections](#) — Indica uma lista de SA ativos com suas relações associadas, transforma-a e opõe-se.

Exemplo de saída de show

Esta seção captura os **show command outputs (resultado do comando show)** no roteador Daphne, quando um **comando ping** é executado no host 13.13.13.4 destinado para o host 12.12.12.13. As saídas no Fred de roteador são igualmente similares. Os parâmetros chaves na saída são indicados em corajoso. Refira o [Troubleshooting de Segurança IP - Compreendendo e usando comandos debug](#) para uma explicação nas saídas do comando.

```

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

```

[Troubleshooting](#)

Use esta seção para resolver problemas de configuração.

[Comandos para Troubleshooting](#)

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- [motor do debug crypto](#) — Indica a informação sobre a crypto-engine que executa a criptografia e o processo de decriptografia.
- [IPsec do debug crypto](#) — Indica as negociações de IPSEC de fase 2.
- [isakmp do debug crypto](#) — Indica as negociações de IKE da fase 1.

[Exemplo de debug](#)

Esta seção captura os **comandos debug** no Roteadores configurado com IPsec, quando um **comando ping** é executado no host 13.13.13.4 destinado para o host 12.12.12.13.

- [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_DISCOVERY (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_DISCOVERY (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#

[Informações Relacionadas](#)

- [IPsec de distribuição](#)
- [Realce do Tunnel Endpoint Discovery](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)