Nota técnica de Troubleshooting de Depurações de IPSec e IKE ASA (Modo Agressivo IKEv1)

Contents

Introduction

Este documento descreve as depurações no Cisco Adaptive Security Appliance (ASA) quando o modo agressivo e a chave pré-compartilhada (PSK) são usados. A tradução de determinadas linhas de debugação na configuração também é discutida. A Cisco recomenda que você tenha um conhecimento básico sobre IPsec e Internet Key Exchange (IKE).

Este documento não discute a passagem de tráfego após o túnel ter sido estabelecido.

Problema principal

As depurações de IKE e IPsec são às vezes criptografadas, mas você pode usá-las para entender problemas com o estabelecimento do túnel VPN IPsec.

Cenário

O modo agressivo é normalmente usado no caso de Easy VPN (EzVPN) com software (Cisco VPN Client) e clientes de hardware (Cisco ASA 5505 Adaptive Security Appliance ou Cisco IOS? roteadores de software), mas somente quando uma chave pré-compartilhada é usada. Ao contrário do modo principal, o modo agressivo consiste em três mensagens.

As depurações são de um ASA que executa o software versão 8.3.2 e atua como um servidor EzVPN. O cliente EzVPN é um cliente de software.

Comandos debug usados

Estes são os comandos debug usados neste documento:

```
debug crypto isakmp 127
debug crypto ipsec 127
```

Configuração do ASA

A configuração do ASA neste exemplo deve ser estritamente básica; nenhum servidor externo é usado.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.48.67.14 255.255.254.0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac

crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

crypto dynamic-map DYN 10 set transform-set TRA
crypto dynamic-map DYN 10 set reverse-route

crypto map MAP 65000 ipsec-isakmp dynamic DYN
crypto map MAP interface outside
crypto isakmp enable outside

crypto isakmp policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
lifetime 86400

username cisco password  cisco
username cisco attributes
vpn-framed-ip-address 192.168.1.100 255.255.255.0

tunnel-group EZ type remote-access
tunnel-group EZ general-attributes
 default-group-policy EZ
tunnel-group EZ ipsec-attributes
 pre-shared-key *****

group-policy EZ internal
group-policy EZ attributes
 password-storage enable
 dns-server value 192.168.1.99
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelall
 split-tunnel-network-list value split
 default-domain value jyoungta-labdomain.cisco.com
```

Depuração

Note: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

Descrição da mensagem do servidor	Debugs		Descrição da mensagem do cliente
	49711:28:30.28908/24/12Gravação=Info/6IKE/0x63000 03B Tentando estabelecer uma conexão com 64.102.156.88. 49811:28:30.29708/24/12Gravo=Depuração/7IKE/0x63 000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_INITIALEvento: EV_INITIATOR 49911:28:30.29708/24/12Gravação=Info/4IKE/0x63000 001 Iniciando a negociação da fase 1 do IKE 50011:28:30.29708/24/12Gravo=Depuração/7IKE/0x63 000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Evento: EV_GEN_DHKEY 50111:28:30.30408/24/12Gravidade=Depuração/7IKE/0 x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Evento: EV_BLD_MSG 50211:28:30.30408/24/12Gravidade=Depuração/7IKE/0 x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Evento: EV_START_RETRY_TMR 50311:28:30.30408/24/12Gravação=Depuração/7IKE/0x 63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Evento: EV_SND_MSG		O modo agressivo é iniciado. Construa AM1. Esse processo inclui: - ISAKMP HDR - Dispositivo de segurança (SA) que contém todos os payloads e propostas de transformação suportados pelo cliente - Carga útil do Key Exchange - ID do iniciador da fase 1 - Nonce
	50411:28:30.30408/24/12Gravação=Informações/4IKE/ 0x63000013 ENVIANDO >>> ISAKMP OAK AG (SA, KE, NON, ID, VID(Xauth), VID(dpd), VID(Frag), VID(Nat-T), VID(Unity)) para 64.102.156.88		Enviar AM1.
	<========== Mensagem agressiva 1 (AM1) ==========		
Receba AM1 do cliente.	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, Mensagem RECEBIDA IKE_DECODE	50611:28:30.33308/24/12Gravação=D epuração/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurStat e: AM_WAIT_MSG2Evento:	Aguarde a resposta do servidor.

	(msgid=0) com payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + FORNECEDOR (13) + FORNECEDOR (13) + FORNECEDOR (13) + FORNECEDOR (13) + FORNECEDOR (13) + NENHUM (0) comprimento total : 849	EV_NO_EVENT	

Processar AM1. Compare as propostas recebidas e as transformações com as já configuradas para correspondências. Configuração relevante: O ISAKMP é ativado na interface e pelo menos uma política é definida que corresponde ao que o cliente enviou:
 	
`crypto isakmp enable outside`
`crypto isakmp policy 10`
`authentication pre-share`
`encryption aes`
`hash sha`
`group 2`
`lifetime 86400`
Grupo de túnel correspondente ao nome de identidade presente:
 	
`tunnel-group EZ type remote-access`
`tunnel-group EZ general-attributes`
`default-group-policy EZ`
`tunnel-group EZ`
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, processando SA payload
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, processando carga útil de ke
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, processando payload ISA_KE
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, processando payload único
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, payload de ID de processamento
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, processando payload VID
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, xauth recebido V6 VID
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, processando payload VID
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, DPD recebido VID
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, processando payload VID
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, VID de fragmentação recebida
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, Peer IKE incluiu sinalizadores de capacidade de fragmentação IKE: Modo principal:Modo TrueAggressive:Falso
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, processando payload VID
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, NAT-Traversal recebido ver 02 VID
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, processando payload VID
	24 de agosto 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, VID do cliente Cisco Unity recebido
	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87,	

ipsec- attributes pre-shared-key cisco	Conexão obtida em tunnel_group ipsec 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, processando o payload SA de IKE 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1]Falha na fase 1:Tipos de atributo incompatíveis para a classe Descrição do grupo:ID do Rcv: Grupo 2Cfgd: Grupo 5 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, IKE SA Proposta nº 1, Transformação	

	nº 5 aceitávelCorresponde à entrada IKE global nº 1	
Construa o AM2. Esse processo inclui: - políticas escolhidas - Diffie-Hellman (DH) - ID do respondedor -auth - Carga útil de detecção de Tradução de Endereço de Rede (NAT - Network Address Translation)	24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo payload SA de ISAKMP 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo a carga útil de ke 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo payload nonce 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, gerando chaves para o Respondedor.. 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo payload de ID 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo a carga útil de hash 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, hash de computação para ISAKMP 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo o payload VID do Cisco Unity 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo o payload V6 VID 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo a carga útil de vid do dpd 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo o NAT-Traversal VID ver 02 payload 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo a carga útil NAT-Discovery 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, computação de hash de descoberta de NAT 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo a carga útil NAT-Discovery 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, computação de hash de descoberta de NAT 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo VID de fragmentação + payload de recursos estendidos 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo payload VID 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, Enviar Altiga/Cisco VPN3000/Cisco ASA GW VID	
Enviar AM2.	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Message (msgid=0) com payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + FORNECEDOR (13) + FORNECEDOR (13) + FORNECEDOR (13) + NAT-D (130) + NAT-D (130) + FORNECEDOR (1) 3) + FORNECEDOR (13) + NENHUM (0) comprimento total: 444	

	========== Mensagem agressiva 2 (AM2) ==========>	
	50711:28:30.40208/24/12Gravação=Info/5IKE/0x63000 02F Pacote ISAKMP recebido: peer = 64.102.156.8 50811:28:30.40308/24/12Gravação=Informações/4IKE/ 0x63000014 RECEBENDO << ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID(Unity), VID(Xauth), VID(dpd), VID(Nat-T), NAT-D, NAT-D, VID(Frag), VID(?) de 64.102.156.8 8 51011:28:30.41208/24/12Gravidade=Depuração/7IKE/0 x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Evento: EV_RCVD_MSG	Receba AM2.
	51111:28:30.41208/24/12Gravação=Informações/5IKE/ 0x63000001 Peer é um peer compatível com Cisco-Unity 51211:28:30.41208/24/12Gravação=Informações/5IKE/ 0x63000001 O par suporta XAUTH 51311:28:30.41208/24/12Gravação=Informações/5IKE/ 0x63000001 O par suporta DPD 51411:28:30.41208/24/12Gravação=Informações/5IKE/ 0x63000001 O colega suporta NAT-T 51511:28:30.41208/24/12Gravação=Informações/5IKE/ 0x63000001 O peer suporta cargas úteis de fragmentação IKE 51611:28:30.41208/24/12Gravidade=Depuração/7IKE/0 x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Evento: EV_GEN_SKEYID 51711:28:30.42208/24/12Gravidade=Depuração/7IKE/0 x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Evento: EV_AUTHENTICATE_PEER 51811:28:30.42208/24/12Gravidade=Depuração/7IKE/0 x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Evento: EV_ADJUST_PORT 51911:28:30.42208/24/12Gravidade=Depuração/7IKE/0 x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Evento: EV_CRYPTO_ATIVE	Processar AM 2.
	52011:28:30.42208/24/12Gravação=Depuração/7IKE/0x 63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5	Construa o AM3. Esse processo inclui a

	R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Evento: EV_BLD_MSG] 52111:28:30.42208/24/12Gravação=Depuração/8IKE/0x63000001 Configuração da ID do fornecedor do IOS iniciada 52211:28:30.42208/24/12Gravação=Informações/6IKE/0x63000001 Configuração de ID de fornecedor do IOS bem-sucedida	autenticação do cliente. Neste momento, todos os dados relevantes para a criptografia já foram trocados.
	52311:28:30.42308/24/12Gravação=Depuração/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Evento: EV_SND_MSG 52411:28:30.42308/24/12Gravação=Informações/4IKE/0x63000013 ENVIANDO >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT, NAT-D, NAT-D, VID(?), VID(Unity)) para 64.102.156.88	Enviar AM3.
	<========== Mensagem agressiva 3 (AM3) ==========	
Receba AM3 do cliente.	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, Mensagem RECEBIDA IKE_DECODE (msgid=0) com payloads : HDR + HASH (8) + NOTIFICAÇÃO (11) + NAT-D (130) + NAT-D (130) + FORNECEDOR (13) + FORNECEDOR (13) + NENHUM (0) comprimento total: 168	
Processar AM 3. Confirme o uso do NAT Transversal (NAT-T). Ambos os lados estão prontos para iniciar a criptografia de tráfego.	24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, processamento de payload de hash 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, hash de computação para ISAKMP 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, processando payload de notificação 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, processando a carga útil NAT-Discovery 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, computação de hash de descoberta de NAT 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, processando a carga útil NAT-Discovery 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, computação de hash de descoberta de NAT 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, processando payload VID 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, Processando payload de ID de fornecedor IOS/PIX (versão: 1.0.0, recursos: 00000408) 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, processando payload VID 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, VID do cliente Cisco Unity recebido	

	24 de agosto 11:31:03 [IKEv1]Grupo = ipsec, IP = 64.102.156.87, detecção automática de NAT Status:extremidade remotaISatrás de um dispositivo NATisend NÃO está atrás de um dispositivo NAT	
Inicie a Fase 1.5 (XAUTH) e solicite as credenciais do usuário.	24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo payload de hash em branco 24 de agosto 11:31:03 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, construindo o payload de hash qm 24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, mensagem de envio IKE_DECODE (msgid=fb709d4d) com payloads : HDR + HASH (8) + ATTR (14) + NONE (0) comprimento total : 72	
	========== XAuth - Solicitação de Credenciais ==========>	
	53511:28:30.43008/24/12Gravação=Informações/4IKE/0x63000014 RECEBENDO << ISAKMP OAK TRANS *(HASH, ATTR) DE 64.102.156.88 53611:28:30.43108/24/12Gravação=Decodificação/11IKE/0x63000001 Cabeçalho ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondente COOKIE:1B301D2DE710EDA0 Próxima Carga:Hash Versão (Hex):10 Tipo de Troca:Transação Sinalizadores:(Criptografia) MessageID(Hex):FB709D4D Comprimento:76 Hash de payload Próximo payload: Atributos Reservado: 00 Comprimento da carga útil: 24 Dados (em hexadecimal): C779D5CBC5C75E3576C478A15A7CAB8A83A232D0 Atributos de payload Próximo payload: Nenhum Reservado: 00 Comprimento da carga útil: 20 Digite: ISAKMP_CFG_REQUEST Reservado: 00 Identifier: 0000 Tipo XAUTH: GENÉRICO Nome de usuário XAUTH: (vazio) Senha do usuário XAUTH: (vazio) 53711:28:30.43108/24/12Gravidade=Depuração/7IKE/0x63000076 Rastreamento NAV->TM:MsgID=FB709D4DCurState: TM_INITIALEvent: EV_RCVD_MSG	Receber solicitação de autenticação. O payload descriptografado mostra campos de nome de usuário e senha vazios.
	53811:28:30.43108/24/12Gravo=Depuração/7IKE/0x63000076 Rastreamento NAV->TM:MsgID=FB709D4DCurState:	Inicie a Fase 1.5 (XAUTH). Inicie o temporizador

	TM_PCS_XAUTH_REQEvent: EV_INIT_XAUTH 53911:28:30.43108/24/12 Gravidade=Depuração/7IKE/0x63000076 Rastreamento NAV->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent: EV_START_RETRY_TMR 54011:28:30.43208/24/12Gravidade=Depuração/7IKE/0x63000076 Rastreamento NAV->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_NO_EVENT 541 11:28:36.41508/24/12Gravo=Depuração/7IKE/0x63000076 Rastreamento NAV->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_RCVD_USER_INPUT	de nova tentativa enquanto aguarda a entrada do usuário. Quando o temporizador de nova tentativa termina, a conexão é automaticamente desconectada.
	54211:28:36.41508/24/12Gravidade=Depuração/7IKE/0x63000076 Rastreamento NAV->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_SND_MSG 54311:28:36.41508/24/12Gravação=Informações/4IKE/0x63000013 ENVIANDO >>> TRANS DE OAK ISAKMP *(HASH, ATTR) para 64.102.156.88 54411:28:36.41508/24/12Gravação=Decodificação/11IKE/0x63000001 Cabeçalho ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondente COOKIE:1B301D2DE710EDA0 Próxima Carga:Hash Versão (Hex):10 Tipo de Troca:Transação Sinalizadores:(Criptografia) MessageID(Hex):FB709D4D Comprimento:85 Hash de payload Próximo payload: Atributos Reservado: 00 Comprimento da carga útil: 24 Dados (em hexadecimal): 1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5 Atributos de payload Próximo payload: Nenhum Reservado: 00 Comprimento da carga útil: 33 Digite: ISAKMP_CFG_REPLY Reservado: 00 Identifier: 0000 Tipo XAUTH: GENÉRICO Nome de usuário XAUTH: (dados não exibidos) Senha do usuário XAUTH: (dados não exibidos)	Quando a entrada do usuário for recebida, envie credenciais de usuário ao servidor. O payload descriptografado mostra os campos de nome de usuário e senha preenchidos (mas ocultos). Solicitação de configuração do modo de envio (vários atributos).
	<========== Xauth - Credenciais do usuário ==========	
Receber credenciais	24 de agosto 11:31:09 [IKEv1]IP = 64.102.156.87,	

de usuário.	Mensagem RECEBIDA IKE_DECODE (msgid=fb709d4d) com payloads : HDR + HASH (8) + ATTR (14) + NENHUM (0) comprimento total: 85 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, process_Attribute(): Insira!	
Processar credenciais de usuário. Verifique as credenciais e gere o modo config payload. Configuração relevante: `username cisco password cisco`	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, IP = 64.102.156.87, atributos Processing MODE_CFG Reply. 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, IKEGetUserAttributes: DNS primário = 192.168.1.99 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, IKEGetUserAttributes: DNS secundário = limpo 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, IKEGetUserAttributes: WINS principal = limpo 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, IKEGetUserAttributes: WINS secundário = limpo 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, IKEGetUserAttributes: lista de túneis divididos = divisão 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, IKEGetUserAttributes: domínio padrão = jyoung-labdomain.cisco.com 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, IKEGetUserAttributes: Compactação de IP = desabilitado 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, IKEGetUserAttributes: Política de tunelamento dividido = Desabilitado 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, IKEGetUserAttributes: Configuração do proxy do navegador = não-modificar 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, IKEGetUserAttributes: Navegador Proxy Ignorar Local = desabilitar 24 de agosto 11:31:09 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Usuário (usuário1) autenticado.	
Enviar resultado de xuath.	24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, construindo payload de hash em branco 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, construindo o payload de hash de qm	

	24 de agosto 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Message (msgid=5b6910ff) com payloads : HDR + HASH (8) + ATTR (14) + NONE (0) comprimento total : 64	
	========== XAuth - Resultado da autorização ==========>	
	54511:28:36.41608/24/12Gravação=Depuração/7IKE/0x63000076 Rastreamento NAV->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_XAUTHREQ_DONE 54611:28:36.41608/24/12Gravação=Depuração/7IKE/0x63000076 Rastreamento NAV->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_NO_EVENT 54711:28:36.42408/24/12Gravação=Info/5IKE/0x6300002F Pacote ISAKMP recebido: peer = 64.102.156.88 54811:28:36.42408/24/12Gravação=Informações/4IKE/0x63000014 RECEBENDO << ISAKMP OAK TRANS *(HASH, ATTR) DE 64.102.156.88 54911:28:36.42508/24/12Gravação=Decodificação/11IKE/0x63000001 Cabeçalho ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondente COOKIE:1B301D2DE710EDA0 Próxima Carga:Hash Versão (Hex):10 Tipo de Troca:Transação Sinalizadores:(Criptografia) MessageID(Hex):5B6910FF Comprimento:76 Hash de payload Próximo payload: Atributos Reservado: 00 Comprimento da carga útil: 24 Dados (em hexadecimal): 7DCF47827164198731639BFB7595F694C9DFE85 Atributos de payload Próximo payload: Nenhum Reservado: 00 Comprimento da carga útil: 12 Digite: ISAKMP_CFG_SET Reservado: 00 Identifier: 0000 Estado XAUTH: Aprovado 55011:28:36.42508/24/12Gravidade=Depuração/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_INITIALEvent: EV_RCVD_MSG 55111:28:36.42508/24/12Gravidade=Depuração/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState:	Receba resultados de autenticação e resultados do processo.

	TM_PCS_XAUTH_SETEvent: EV_INIT_XAUTH 55211:28:36.42508/24/12Gravidade=Depuração/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_CHK_AUTH_RESULT	
	55311:28:36.42508/24/12Gravação=Informações/4IKE/0x63000013 ENVIANDO >>> TRANS DE OAK ISAKMP *(HASH, ATTR) para 64.102.156.88	Resultado ACK.
	<========== Xauth - Confirmação ==========	
Receber e processar ACK; nenhuma resposta do servidor.	24 de agosto 11:31:09 [IKEv1]IP = 64.102.156.87, Mensagem RECEBIDA IKE_DECODE (msgid=5b6910ff) com payloads : HDR + HASH (8) + ATTR (14) + NONE (0) comprimento total : 60 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, process_Attribute(): Insira! 24 de agosto 11:31:09 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Processando atributos cfg ACK	
	55511:28:36.42608/24/12Gravidade=Depuração/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_XAUTH_DONE_SUC 55611:28:36.42608/24/12Gravidade=Depuração/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_NO_EVENT 55711:28:36.42608/24/12Gravo=Depuração/7IKE/0x63000076 Rastreamento NAV->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_TERM_REQUEST 55811:28:36.42608/24/12Gravo=Depuração/7IKE/0x63000076 Rastreamento NAV->TM:MsgID=FB709D4DCurState: TM_FREEvaso: EV_REMOVE 55911:28:36.42608/24/12Gravação=Depuração/7IKE/0x63000076 Rastreamento NAV->TM:MsgID=FB709D4DCurState: TM_FREEvaso: EV_NO_EVENT 56011:28:36.42608/24/12Gravidade=Depuração/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_XAUTH_PROGEvent: EV_XAUTH_DONE_SUC 56111:28:38.40608/24/12Gravidade=Depuração/8IKE/0x6300004C Iniciando temporizador DPD para IKE SA (I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0) sa->estado = 1, sa-	Gerar solicitação mode-config. O payload descriptografado mostra os parâmetros solicitados do servidor.

	>dpd.preocupado_freq(mSec) = 5000 56211:28:38.40608/24/12Gravo=Depuração/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_MODECFG 56311:28:38.40608/24/12Gravo=Depuração/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_NO_EVENT 56411:28:38.40608/24/12Gravo=Depuração/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_INITIALEvent: EV_INIT_MODECFG 56511:28:38.40808/24/12Gravação=Info/5IKE/0x6300005E Cliente enviando uma solicitação de firewall ao concentrador 56611:28:38.40908/24/12Gravo=Depuração/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_START_RETRY_TMR	
	56711:28:38.40908/24/12Gravo=Depuração/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_SND_MSG 56811:28:38.40908/24/12Gravidade=Info/4IKE/0x63000013 ENVIANDO >>> TRANS DE OAK ISAKMP *(HASH, ATTR) para 64.102.156.88 56911:28:38.62708/24/12Gravação=Decodificação/11IKE/0x63000001 Cabeçalho ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondente COOKIE:1B301D2DE710EDA0 Próxima Carga:Hash Versão (Hex):10 Tipo de Troca:Transação Sinalizadores:(Criptografia) MessageID(Hex):84B4B653 Comprimento:183 Hash de payload Próximo payload: Atributos Reservado: 00 Comprimento da carga útil: 24 Dados (em hexadecimal): 81BFBF6721A744A815D69A315EF4AAA571D6B687 Atributos de payload Próximo payload: Nenhum	Enviar solicitação mode-config.

	Reservado: 00 Comprimento da carga útil: 131 Digite: ISAKMP_CFG_REQUEST Reservado: 00 Identifier: 0000 Endereço IPv4: (vazio) Máscara de rede IPv4: (vazio) DNS IPv4: (vazio) NBNS IPv4 (WINS): (vazio) Expiração do endereço: (vazio) Ramal da Cisco: Banner: (vazio) Ramal da Cisco: Salvar PWD: (vazio) Ramal da Cisco: Nome de domínio padrão: (vazio) Ramal da Cisco: Dividir inclusão: (vazio) Ramal da Cisco: Dividir nome DNS: (vazio) Ramal da Cisco: Do PFS: (vazio) Desconhecido: (vazio) Ramal da Cisco: Servidores de backup: (vazio) Ramal da Cisco: Desconexão da remoção do cartão inteligente: (vazio) Versão do aplicativo: Cisco Systems VPN Client 5.0.07.0290:WinNT Ramal da Cisco: Tipo de firewall: (vazio) Ramal da Cisco: Nome de host DNS dinâmico: CAIXA DE TRABALHO ATBASU		
	<========== Solicitação de configuração do modo ==========		
Receber solicitação mode-config.	24 de agosto 11:31:11 [IKEv1]IP = 64.102.156.87, Mensagem RECEBIDA IKE_DECODE (msgid=84b4b653) com payloads : HDR + HASH (8) + ATTR (14) + NONE (0) comprimento total : 183 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, process_Attribute(): Insira!	57011:28:38.62808/24/12Gravação= Depuração/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvento: EV_NO_EVENT	Aguarde a resposta do servidor.

Processar solicitação mode-config. Muitos desses valores são geralmente configurados na política de grupo. No entanto, como o servidor neste exemplo tem uma configuração muito básica, você não os vê aqui.	24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Processando atributos de solicitação cfg 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação de endereço IPV4 recebida! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação recebida para a máscara de rede IPV4! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação recebida para o endereço do servidor DNS! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação recebida para o endereço do servidor WINS! 24 de agosto 11:31:11 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, atributo do modo de transação não suportado recebido: 5 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação de Banner recebida! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação recebida para a configuração Salvar PW! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação recebida para o nome de domínio padrão! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação recebida para a lista de túneis divididos! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação recebida para DNS dividido! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação recebida para configuração PFS! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação recebida para a configuração do proxy do navegador do cliente! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação recebida para backup da lista de peer ip-sec! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87,	

	MODE_CFG: Solicitação recebida para a configuração de desconexão da remoção do cartão inteligente do cliente! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação recebida para a versão do aplicativo! 24 de agosto 11:31:11 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Tipo de cliente: Versão do aplicativo WinNTClient: 5.0.07.0290 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: Solicitação recebida para FWTYPE! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, MODE_CFG: A solicitação recebida para o nome de host DHCP para DDNS é: CAIXA DE TRABALHO ATBASU!	
Construa a resposta mode-config com todos os valores configurados. Configuração relevante: Observe que, nesse caso, o usuário sempre recebe o mesmo IP. username cisco attributes **vpn-framed-ip-address 192.168.1.100 255.255.255.0** group-policy EZ internal group-policy EZ attributes password-storage enabledns-server value 192.168.1.129 vpn-tunnel-protocol ikev1 split-tunnel-policy tunnelall split-tunnel-network-list value split default-domain value jyoungta-labdomain.cisco.com	24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Endereço IP obtido (192.168.1.100) antes de iniciar o modo Cfg (XAuth ativado) 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, enviando máscara de sub-rede (255.255.255.0) para o cliente remoto 24 de agosto 11:31:11 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Endereço IP privado atribuído 192.168.1.100 para usuário remoto 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, construindo payload de hash em branco 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, construct_cfg_set: domínio padrão = jyoung-labdomain.cisco.com 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Enviar atributos do proxy do navegador do cliente! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Proxy do navegador definido como Sem modificação. Os dados do proxy do navegador NÃO serão incluídos na resposta mode-cfg 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Enviar desconexão de remoção de cartão inteligente da Cisco!! 24 de agosto 11:31:11 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, construindo o payload de hash de qm	
Enviar resposta de configuração de modo.	24 de agosto 11:31:11 [IKEv1]IP = 64.102.156.87, mensagem de envio IKE_DECODE (msgid=84b4b653) com payloads : HDR + HASH (8) + ATTR (14) + NONE	

	(0) comprimento total : 215		
	========== Resposta de configuração do modo ==========>		
	57111:28:38.63808/24/12Gravação=Info/5IKE/0x63000 02F Pacote ISAKMP recebido: peer = 64.102.156.88 57211:28:38.63808/24/12Gravação=Informações/4IKE/ 0x63000014 RECEBENDO << ISAKMP OAK TRANS *(HASH, ATTR) DE 64.102.156.88 57311:28:38.63908/24/12Gravação=Decodificação/11IK E/0x63000001 Cabeçalho ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondente COOKIE:1B301D2DE710EDA0 Próxima Carga:Hash Versão (Hex):10 Tipo de Troca:Transação Sinalizadores:(Criptografia) MessageID(Hex):84B4B653 Comprimento:220 Hash de payload Próximo payload: Atributos Reservado: 00 Comprimento da carga útil: 24 Dados (em hexadecimal): 6DE2E70ACF6B185846BC62E590C00A66745D14D Atributos de payload Próximo payload: Nenhum Reservado: 00 Comprimento da carga útil: 163 Digite: ISAKMP_CFG_REPLY Reservado: 00 Identifier: 0000 Endereço IPv4: 192.168.1.100 Máscara de rede IPv4: 255.255.255.0 DNS IPv4: 192.168.1.99 Ramal da Cisco: Salvar PWD: No Ramal da Cisco: Nome de domínio padrão: jyoungta-labdomain.cisco.com Ramal da Cisco: Do PFS: No Versão do aplicativo: Cisco Systems, Inc ASA5505 Versão 8.4(4)1 construída por construtores em 14 de junho de 2012 11:20 Ramal da Cisco: Desconexão da remoção do cartão inteligente: Yes		Receber valores de parâmetro mode-config do servidor.
A fase 1 é concluída no servidor. Iniciar o processo de modo rápido (QM).	24 de agosto 11:31:13 [DECODE IKEv1]IP = 64.102.156.87, Respondedor IKE iniciando	57411:28:38.63908/24/12Gravação= Depuração/7IKE/0x63000076 NAV Trace- >TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvento: EV_RCVD_MSG 57511:28:38.63908/24/12Gravação=	Processar parâmetros e se configurar de acordo.

	QM: id da msg = 0e83792e 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, processamento de Atraso no Modo Rápido, Exportação de Cert/Trans/RM DSID em andamento 24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, ARP Gratuito enviado para 192.168.1.100 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, retomar o processamento do modo rápido, Cert/Trans Exch/RM DSID concluído 24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, FASE 1 CONCLUÍDA	Info/5IKE/0x63000010 MODE_CFG_REPLY: Atributo = INTERNAL_IPV4_ADDRESS:, valor = 192.168.1.100 57611:28:38.63908/24/12Gravação=Informações/5IKE/0x63000010 MODE_CFG_REPLY: Atributo = INTERNAL_IPV4_NETMASK:, valor = 255.255.255.0 57711:28:38.63908/24/12Gravação=Info/5IKE/0x63000010 MODE_CFG_REPLY: Atributo = INTERNAL_IPV4_DNS(1): , valor = 192.168.1.99 57811:28:38.63908/24/12Gravação=Info/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = MODECFG_UNITY_SAVEPWD: , valor = 0x00000000 57911:28:38.63908/24/12Gravação=Info/5IKE/0x6300000E MODE_CFG_REPLY: Atributo = MODECFG_UNITY_DEFDOMAIN: , valor = jyoung-labdomain.cisco.com 58011:28:38.63908/24/12Gravação=Info/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = MODECFG_UNITY_PFS: , valor = 0x00000000 58111:28:38.63908/24/12Gravação=Info/5IKE/0x6300000E MODE_CFG_REPLY: Atributo = APPLICATION_VERSION, valor = Cisco Systems, Inc ASA5505 versão 8.4(4)1 criada por construtores em Tu 14-jun-12 11:20 58211:28:38.63908/24/12Gravação=Info/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = MODECFG_UNITY_SMARTCARD_REMOVAL_DISCONNECT: , valor = 0x00000001 58311:28:38.63908/24/12Gravação=Info/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = Recebido e usando NAT-T número da porta , valor = 0x00001194 58411:28:39.36708/24/12Gravação=Depuração/9IKE/0x63000093 O valor para o parâmetro ini EnableDNSRedirection é 1 58511:28:39.36708/24/12Gravação=	

		Depuração/7IKE/0x63000076 NAV Trace- >TM:MsgID=84B4B653CurState: TM_MODECFG_DONEEvent: EV_MODECFG_DONE_SUC	
Construir e enviar DPD para o cliente.	24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, tipo de manutenção de atividade para esta conexão: DPD 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, iniciando o temporizador de chave P1: 82080 segundos. 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, enviando mensagem de notificação 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, construindo payload de hash em branco 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, construindo o payload de hash de qm 24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, mensagem de envio IKE_DECODE (msgid=be8f7821) com payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) comprimento total : 92	
	========== Detecção de Peer Morto (DPD) ==========>		
	58811:28:39.79508/24/12Gravo=Depuração/7IKE/0x63000015 intf_data: lcl=0x0501A8C0, mask=0x00FFFFF, bcast=0xFF01A8C0, bcast_vra=0xFF07070A 58911:28:39.79508/24/12Gravo=Depuração/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_P2 59011:28:39.79508/24/12Gravação=Informações/4IKE/0x63000056 Recebida uma solicitação de chave do driver: IP local = 192.168.1.100, IP GW = 64.102.156.88, IP remoto = 0.0.0.0 59111:28:39.79508/24/12Gravo=Depuração/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_ATIVEEvento: EV_NO_EVENT 59211:28:39.79508/24/12Gravo=Depuração/7IKE/0x63000076 Rastreamento NAV->QM:MsgID=0E83792ECurState: QM_INITIALEvent: EV_INITIATOR 59311:28:39.79508/24/12Gravo=Depuração/7IKE/0x63000076 Rastreamento NAV->QM:MsgID=0E83792ECurState: Evento QM_BLD_MSG1: EV_CHK_PFS 59411:28:39.79608/24/12Gravo=Depuração/7IKE/0x63	Iniciar QM, Fase 2. Construir QM1. Esse processo inclui: - Hash - SA com todas as propostas da Fase 2 apoiadas pelo cliente, tipo de túnel e criptografia - Nonce - ID do cliente - IDs de proxy

	000076 Rastreamento NAV->QM:MsgID=0E83792ECurState: Evento QM_BLD_MSG1: EV_BLD_MSG 59511:28:39.79608/24/12Gravo=Depuração/7IKE/0x63 000076 Rastreamento NAV->QM:MsgID=0E83792ECurState: Evento QM_SND_MSG1: EV_START_RETRY_TMR	
	59611:28:39.79608/24/12Gravo=Depuração/7IKE/0x63 000076 Rastreamento NAV->QM:MsgID=0E83792ECurState: Evento QM_SND_MSG1: EV_SND_MSG 59711:28:39.79608/24/12Gravação=Informações/4IKE/ 0x63000013 ENVIANDO >>> ISAKMP OAK QM *(HASH, SA, NON, ID) para 64.102.156.88	Enviar QM1.
	<========== Mensagem do Modo Rápido 1 (QM1) ==========	
Receber QM1.	24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, Mensagem RECEBIDA IKE_DECODE (msgid=e83792e) com payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) comprimento total : 1026	
Processar QM1. Configuração relevante: `crypto dynamic-map DYN 10 set transform-set TRA`	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, processando a carga útil de hash 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, processando o payload SA 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, processando payload único 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, payload de ID de processamento 24 de agosto 11:31:13 [IKEv1 DECODE]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, ID_IPV4_ADDR ID recebida 192.168.1.100 24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Dados do host do proxy remoto recebidos no payload do ID:Endereço 192.168.1.100, Protocolo 0, Porta 0 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, payload de ID de processamento 24 de agosto 11:31:13 [IKEv1 DECODE]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, ID_IPV4_ADDR_SUBNET ID recebido—0.0.0.0—0.0.0.0 24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Dados da sub-rede do Proxy IP local recebidos no ID Payload: Endereço 0.0.0.0, Máscara 0.0.0, Protocolo 0, Porta 0	

	24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, QM IsRekeyed old sa não encontrado por addr 24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, verificação de mapa de criptografia estático, mapa de verificação = mapa de saída, seq = 10... 24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Verificação de mapa de criptografia estático com aprovação: Entrada de mapa de criptografia incompleta! 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Selecionando somente os modos UDP-Encapsulated-Tunnel e UDP-Encapsulated-Transport definidos pelo NAT-Traversal 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Selecionando somente os modos UDP-Encapsulated-Tunnel e UDP-Encapsulated-Transport definidos pelo NAT-Traversal 24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Peer remoto IKE configurado para mapa de criptografia: out-dyn-map 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, processando o payload SA do IPSec	

Construa o QM2. Configuração relevante:
 	
`tunnel-group EZ type` **`remote-access`** *`! (tunnel type ra = tunnel type remote-access)`*
`crypto ipsec transform-set TRA` **`esp-aes esp-sha-hmac`**
`crypto ipsec security-association` **`lifetime seconds 28800`**
`crypto ipsec security-association lifetime kilobytes 4608000`
`crypto dynamic-map DYN 10 set transform-set TRA`
`crypto map MAP 65000 ipsec-isakmp dynamic DYN`
`crypto map MAP interface outside`
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Proposta de SA IPSec nº 12, Transformação nº 1 aceitávelCorresponde à entrada de SA global IPSec nº 10
	24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, IKE: solicitando SPI!
	IPSEC: Nova SA embrionária criada em 0xcfdffc90, SCB: 0xCFDFB58, Direção: entrada
	SPI: 0x9E18ACB2
	ID da sessão: 0x00138000
	Número VPIF: 0x0000004
	Tipo de túnel: ra
	Protocolo: esp
	Duração: 240 segundos
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, IKE obteve SPI do mecanismo de chave: SPI = 0x9e18acb2
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, construindo o modo rápido de Oakley
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, construindo payload de hash em branco
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec,	

	nome de usuário = usuário1, IP = 64.102.156.87, construindo o payload SA de IPSec 24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, sobrepondo a duração de rechaveamento de IPSec do iniciador de 2147483 a 86400 segundos 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, construindo o payload de IPSec nonce 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, construindo ID de proxy 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Transmitindo ID do proxy: Host remoto: 192.168.1.100Protocolo 0Porta 0 Sub-rede local:0.0.0.0mask 0.0.0.0 Protocolo 0Porta 0 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, enviando notificação RESPOSTA LIFETIME ao iniciador 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, construindo o payload de hash de qm	
Enviar QM2.	24 de agosto 11:31:13 [IKEv1 DECODE]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Respondedor IKE enviando o segundo pacote QM: id da msg = 0e83792e 24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Message (msgid=e83792e) com payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFICAÇÃO (11) + NENHUM (0) comprimento total : 184	
	========== Mensagem do Modo Rápido 2 (QM2) ==========>	
	60811:28:39.96208/24/12Gravação=Info/4IKE/0x63000014 RECEBENDO << ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) de 64.102.156.88	Receber QM2.
	60911:28:39.96408/24/12Gravação=Decodificação/11IKE/0x63000001 Cabeçalho ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondente COOKIE:1B301D2DE710EDA0 Próxima Carga:Hash Versão (Hex):10 Tipo de troca:Modo rápido Sinalizadores:(Criptografia) MessageID(Hex):E83792E Comprimento:188 Hash de payload Próximo payload: Associação de segurança Reservado: 00	Processar QM2. O payload descriptografado mostra as propostas escolhidas.

	Comprimento da carga útil: 24 Dados (em hexadecimal): CABF38A62C9B88D1691E81F3857D6189534B2EC0 Associação de segurança de payload Próximo payload: Nonce Reservado: 00 Comprimento da carga útil: 52 DOI: IPsec Situação: (SIT_IDENTITY_ONLY) Proposta de payload Próximo payload: Nenhum Reservado: 00 Comprimento da carga útil: 40 Nº da proposta: 1 ID do protocolo: PROTO_IPSEC_ESP Tamanho do SPI: 4 Nº de transformações: 1 SPI: 9E18ACB2 Transformação de payload Próximo payload: Nenhum Reservado: 00 Comprimento da carga útil: 28 Nº da transformação: 1 ID da transformação: ESP_3DES Reservado2: 0000 Tipo de vida: Segundos Duração (Hex): 0020C49B Modo de encapsulamento: Túnel UDP Algoritmo de autenticação: SHA1 Carga útil Nonce Próximo payload: Identificação Reservado: 00 Comprimento da carga útil: 24 Dados (em hexadecimal): 3A079B75DA512473706F235EA3FCA61F1D15D4CD Identificação de payload Próximo payload: Identificação Reservado: 00 Comprimento da carga útil: 12 Tipo de ID: Endereço IPv4 ID do protocolo (UDP/TCP, etc...): 0 Porta: 0 &Dois pontos de ID; 192.168.1.100 Identificação de payload Próximo payload: Notificação Reservado: 00 Comprimento da carga útil: 16 Tipo de ID: Sub-rede IPv4 ID do protocolo (UDP/TCP, etc...): 0 Porta: 0 &Dois pontos de ID; 0.0.0.0/0.0.0.0	

	Notificação de payload Próximo payload: Nenhum Reservado: 00 Comprimento da carga útil: 28 DOI: IPsec ID do protocolo: PROTO_IPSEC_ESP Tamanho do Spi: 4 Tipo de notificação: STATUS_RESP_LIFETIME SPI: 9E18ACB2 &Dois pontos; Tipo de vida: Segundos Duração (Hex): 00015180	
	61011:28:39.96508/24/12Gravação=Depuração/7IKE/0x63000076 Rastreamento NAV->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Evento: EV_RCVD_MSG 61111:28:39.96508/24/12Gravação=Informações/5IKE/0x63000045 A notificação RESPONDER-LIFETIME tem valor de 86400 segundos 61211:28:39.96508/24/12Gravação=Depuração/7IKE/0x63000076 Rastreamento NAV->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Evento: EV_CHK_PFS 61311:28:39.96508/24/12Gravação=Depuração/7IKE/0x63000076	Processar QM2.
	Rastreamento NAV->QM:MsgID=0E83792ECurState: QM_BLD_MSG3Evento: EV_BLD_MSG 61411:28:39.96508/24/12Gravação=Depuração/7IKE/0x63000076 Cabeçalho ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Respondente COOKIE:1B301D2DE710EDA0 Próxima Carga:Hash Versão (Hex):10 Tipo de troca:Modo rápido Sinalizadores:(Criptografia) MessageID(Hex):E83792E Comprimento:52 Hash de payload Próximo payload: Nenhum Reservado: 00 Comprimento da carga útil: 24 Dados (em hexadecimal): CDDC20D91EB4B568C826D6A5770A5CF020141236	Construa QM3. Carga descriptografada para QM3 mostrada aqui. Este processo inclui hash.
	61511:28:39.96508/24/12Gravo=Depuração/7IKE/0x63000076 Rastreamento NAV->QM:MsgID=0E83792ECurState: QM_SND_MSG3Evento: EV_SND_MSG 61611:28:39.96508/24/12Gravação=Info/4IKE/0x63000013 ENVIANDO >>> ISAKMP OAK QM *(HASH) para	Enviar QM3. O cliente agora está pronto para criptografar e descriptografar.

	64.102.156.88	
	<========== Mensagem do Modo Rápido 3 (QM3) ==========	
Receber QM3.	24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, Mensagem RECEBIDA IKE_DECODE (msgid=e83792e) com payloads : HDR + HASH (8) + NONE (0) comprimento total : 52	

Processar QM3. Crie os índices de parâmetros de segurança (SPIs) de entrada e saída. Adicione uma rota estática para o host. Configuração relevante:
 	
`crypto ipsec transform-set TRA esp-aes esp-sha-hmac`
`crypto ipsec security-association lifetime seconds 28800`
`crypto ipsec security-association lifetime kilobytes 4608000`
`crypto dynamic-map DYN 10 set transform-set TRA`
`crypto dynamic-map DYN 10` **`set reverse-route`**
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, processando a carga útil de hash
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, carregando todas as SAs IPSEC
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, gerando chave de modo rápido!
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, pesquisa de regra de criptografia NP para mapa de criptografia out-dyn-map 10 ACL correspondente Desconhecido: retornado cs_id=cc107410; rule=00000000
	24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, gerando chave de modo rápido!
	IPSEC: Nova SA embrionária criada em 0xccc9ed60, SCB: 0xCF7F59E0,
	Direção: saída
	SPI: 0xC055290A
	ID da sessão: 0x00138000
	Número VPIF: 0x0000004
	Tipo de túnel: ra
	Protocolo: esp
	Duração: 240 segundos
	IPSEC: Atualização de OBSA do host concluída, SPI 0xC055290A
	IPSEC: Criando contexto de VPN de saída, SPI 0xC055290A
	Flags: 0x00000025
	SA: 0xccc9ed60
	SPI: 0xC055290A
	MTU: 1500 bytes
	VCID: 0x00000000
	Correspondente: 0x00000000
	SCB: 0xA5922B6B
	Canal: 0xc82afb60
	IPSEC: Contexto VPN de saída concluído, SPI 0xC055290A
	Identificador de VPN: 0x0015909c
	IPSEC: Nova regra de criptografia de saída, SPI 0xC055290A
	Endereço Src: 0.0.0.0
	Máscara de Src: 0.0.0.0	

	Dst addr: 192.168.1.100 Máscara de dia: 255.255.255.255 Portas Src Superior: 0 Inferior: 0 Op: ignore Portas Dst Superior: 0 Inferior: 0 Op: ignore Protocolo: 0 Usar protocolo: falso SPI: 0x00000000 Usar SPI: falso IPSEC: Regra de criptografia de saída concluída, SPI 0xC055290A ID da regra: 0xcb47a710 IPSEC: Nova regra de permissão de saída, SPI 0xC055290A Endereço Src: 64.102.156.88 Máscara de Src: 255.255.255.255 Dst addr: 64.102.156.87 Máscara de dia: 255.255.255.255 Portas Src Superior: 4500 Inferior: 4500 Op: igual Portas Dst Superior: 58506 Inferior: 58506 Op: igual Protocolo: 17 Usar protocolo: verdadeiro SPI: 0x00000000 Usar SPI: falso IPSEC: Regra de permissão de saída concluída, SPI 0xC055290A ID da regra: 0xcdf3cfa0 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, pesquisa de regra de criptografia NP para mapa de criptografia out-dyn-map 10 ACL correspondente Desconhecido: retornado cs_id=cc107410; rule=00000000 24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Negociação de segurança concluída para usuário (usuário1)Respondedor, SPI de entrada = 0x9e18acb2, Saída SPI = 0xc055290a 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, nome de usuário = usuário1, IP = 64.102.156.87, IKE recebeu uma mensagem KEY_ADD para SA: SPI =	

	0xc055290a IPSEC: Atualização IBSA do host concluída, SPI 0x9E18ACB2 IPSEC: Criando contexto de VPN de entrada, SPI 0x9E18ACB2 Flags: 0x00000026 SA: 0xcfdffc90 SPI: 0x9E18ACB2 MTU: 0 bytes VCID: 0x00000000 Correspondente: 0x0015909C SCB: 0xA5672481 Canal: 0xc82afb60 IPSEC: Contexto VPN de entrada concluído, SPI 0x9E18ACB2 Identificador de VPN: 0x0016219c IPSEC: Atualização do contexto de VPN de saída 0x0015909C, SPI 0xC055290A Flags: 0x00000025 SA: 0xccc9ed60 SPI: 0xC055290A MTU: 1500 bytes VCID: 0x00000000 Correspondente: 0x0016219C SCB: 0xA5922B6B Canal: 0xc82afb60 IPSEC: Contexto VPN de saída concluído, SPI 0xC055290A Identificador de VPN: 0x0015909c IPSEC: Regra interna de saída concluída, SPI 0xC055290A ID da regra: 0xcb47a710 IPSEC: Regra SPD externa de saída concluída, SPI 0xC055290A ID da regra: 0xcdf3cfa0 IPSEC: Nova regra de fluxo de túnel de entrada, SPI 0x9E18ACB2 Endereço Src: 192.168.1.100 Máscara de Src: 255.255.255.255 Dst addr: 0.0.0.0 Máscara de dia: 0.0.0.0 Portas Src Superior: 0 Inferior: 0 Op: ignore Portas Dst Superior: 0 Inferior: 0 Op: ignore Protocolo: 0 Usar protocolo: falso SPI: 0x00000000 Usar SPI: falso	

	IPSEC: Regra de fluxo de túnel de entrada concluída, SPI 0x9E18ACB2 ID da regra: 0xcdf15270 IPSEC: Nova regra de descriptografia de entrada, SPI 0x9E18ACB2 Endereço Src: 64.102.156.87 Máscara de Src: 255.255.255.255 Dst addr: 64.102.156.88 Máscara de dia: 255.255.255.255 Portas Src Superior: 58506 Inferior: 58506 Op: igual Portas Dst Superior: 4500 Inferior: 4500 Op: igual Protocolo: 17 Usar protocolo: verdadeiro SPI: 0x00000000 Usar SPI: falso IPSEC: Regra de descriptografia de entrada concluída, SPI 0x9E18ACB2 ID da regra: 0xce03c2f8 IPSEC: Nova regra de permissão de entrada, SPI 0x9E18ACB2 Endereço Src: 64.102.156.87 Máscara de Src: 255.255.255.255 Dst addr: 64.102.156.88 Máscara de dia: 255.255.255.255 Portas Src Superior: 58506 Inferior: 58506 Op: igual Portas Dst Superior: 4500 Inferior: 4500 Op: igual Protocolo: 17 Usar protocolo: verdadeiro SPI: 0x00000000 Usar SPI: falso IPSEC: Regra de permissão de entrada concluída, SPI 0x9E18ACB2 ID da regra: 0xcf6f58c0 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Pitcher: KEY_UPDATE recebido, spi 0x9e18acb2 24 de agosto 11:31:13 [IKEv1 DEBUG]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, iniciando o temporizador de chave P2: 82080 segundos. 24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, Adicionando	

	rota estática para o endereço do cliente: 192.168.1.100	
Fase 2 concluída. Ambos os lados estão criptografando e descriptografando agora.	24 de agosto 11:31:13 [IKEv1]Grupo = ipsec, Nome de usuário = usuário1, IP = 64.102.156.87, FASE 2 CONCLUÍDA (msgid=0e83792e)	
Para clientes de hardware, é recebida mais uma mensagem em que o cliente envia informações sobre si mesmo. Se você olhar com atenção, deverá encontrar o nome de host do cliente EzVPN, o software que é executado no cliente e o local e o nome do software	24 de agosto 11:31:13 [IKEv1]: IP = 10.48.66.23, Mensagem RECEBIDA IKE_DECODE (msgid=91facca9) com payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) comprimento total : 184 24 de agosto 11:31:13 [DEPURAÇÃO IKEv1]: Grupo = EZ, nome de usuário = cisco, IP = 10.48.66.23, processamento de payload de hash 24 de agosto 11:31:13 [DEPURAÇÃO IKEv1]: Grupo = EZ, nome de usuário = cisco, IP = 10.48.66.23, processando payload de notificação 24 de agosto 11:31:13 [DECODO IKEv1]: DESCRITOR OBSOLETO - ÍNDICE 1 24 de agosto 11:31:13 [DECODO IKEv1]: 0000 : 0000000 7534000B 62736E73 2D383731 ....u4.**bsns-871** 0010 : 2D332E75 32000943 6973636F 20383731 **-3**.u2..**Cisco 871** 0020 : 7535000B 46484B30 39343431 32513675 u5.FHK094412Q6u 0030 : 36000932 32383538 39353638 75390009 6.228589568u9.. 0040 : 31343532 3136331 32753300 2B666C61 145216312u3.+**fla** 0050 : 73683A63 3837302D 61647669 70736572 **sh:c870-advipser** 0060 : 76696365 736B392D 6D7A2E31 32342D32 **vicesk9-mz.124-2** 0070 : 302E5435 2E62696E **0.T5.bin** 24 de agosto 11:31:13 [DEPURAÇÃO IKEv1]: Grupo = EZ, nome de usuário = cisco, IP = 10.48.66.23, processando hash PSK 24 de agosto 11:31:13 [IKEv1]: Grupo = EZ, nome de usuário = cisco, IP = 192.168.1.100, tamanho de hash PSK inconsistente 24 de agosto 11:31:13 [DEPURAÇÃO IKEv1]: Grupo = EZ, nome de usuário = cisco, IP = 10.48.66.23, Falha na verificação de hash de PSK!	

Verificação de túnel

ISAKMP

A saída do comando **sh cry isa sa det** é:

```
 Active SA: 1
 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.48.66.23
 Type : user Role : responder
 Rekey : no State : AM_ACTIVE
 Encrypt : aes Hash : SHA
 Auth : preshared Lifetime: 86400
 Lifetime Remaining: 86387
 AM_ACTIVE - aggressive mode is active.
```

IPsec

Como o Internet Control Message Protocol (ICMP) é usado para disparar o túnel, somente uma SA IPsec está ativa. O Protocolo 1 é ICMP. Observe que os valores de SPI diferem dos negociados nas depurações. Este é, de fato, o mesmo túnel após a chave da Fase 2.

A saída do comando **sh crypto ipsec sa** é:

```
interface: outside
 Crypto map tag: DYN, seq num: 10, local addr: 10.48.67.14

 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 remote ident (addr/mask/prot/port): (192.168.1.100/255.255.255.255/0/0)
 current_peer: 10.48.66.23, username: cisco
 dynamic allocated peer ip: 192.168.1.100

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
 #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.48.67.14/0, remote crypto endpt.: 10.48.66.23/0
 path mtu 1500, ipsec overhead 74, media mtu 1500
 current outbound spi: C4B9A77C
 current inbound spi : EA2B6B15

 inbound esp sas:
 spi: 0xEA2B6B15 (3928714005)
 transform: esp-aes esp-sha-hmac no compression
 in use settings ={RA, Tunnel, }
 slot: 0, conn_id: 425984, crypto-map: DYN
 sa timing: remaining key lifetime (sec): 28714
 IV size: 16 bytes
 replay detection support: Y
 Anti replay bitmap:
 0x00000000 0x0000003F
 outbound esp sas:
 spi: 0xC4B9A77C (3300501372)
 transform: esp-aes esp-sha-hmac no compression
 in use settings ={RA, Tunnel, }
 slot: 0, conn_id: 425984, crypto-map: DYN
 sa timing: remaining key lifetime (sec): 28714
```

```
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

Informações Relacionadas

- Artigo da Wikipedia sobre IPsec
- Solução de problemas de IPsec: Entendendo e usando comandos debug
- Suporte Técnico e Documentação - Cisco Systems