O IPsec ASA e o IKE debugam (a Nota Técnica do Troubleshooting do modo assertivo IKEv1)

Índice

[Introdução](#)
[Edição de núcleo](#)
[Cenário](#)
[comandos debug usados](#)
[Configuração ASA](#)
[Depuração](#)
[Verificação do túnel](#)
[ISAKMP](#)
[IPsec](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve debuga na ferramenta de segurança adaptável de Cisco (ASA) quando o modo assertivo e a chave pré-compartilhada (PSK) são usados. A tradução de determinadas linhas de debugação na configuração também é discutida. Cisco recomenda-o tem um conhecimento básico do IPsec e do Internet Key Exchange (IKE).

Este documento não discute passar o tráfego depois que o túnel foi estabelecido.

Edição de núcleo

O IKE e o IPsec debugam são às vezes enigmáticos, mas você pode usá-lo a fim compreender problemas com estabelecimento de túnel do IPSec VPN.

Cenário

O modo assertivo é usado tipicamente em caso de VPN fácil (EzVPN) com software (Cisco VPN Client) e clientes da ferragem (ferramenta de segurança ou Cisco IOS adaptável de Cisco ASA 5505? Roteadores de software), mas somente quando uma chave pré-compartilhada for usada. O modo do principal diferente, modo assertivo consiste em três mensagens.

Debuga são de um ASA que execute a versão de software 8.3.2 e atue como um servidor de 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 ASA

A configuração ASA neste exemplo é significada ser restritamente básica; nenhum servidor interno 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

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar

comandos **debug**.

Descrição de mensagem do server	Debugs		Descrição de mensagem de cliente
	49711:28:30.28908/24/12Sev=Info/6IKE/0x6300003B Tentativa estabelecer uma conexão com 64.102.156.88. 49811:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_INITIALEvent: EV_INITIATOR 49911:28:30.29708/24/12Sev=Info/4IKE/0x63000001 Começando a negociação da fase 1 IKE 50011:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_GEN_DHKEY 50111:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_BLD_MSG 50211:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_START_RETRY_TMR 50311:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_SND_MSG		Começos do modo assertivo. Construção AM1. Este processo inclui: - ISAKMP HDR - A ferramenta de segurança (SA) que contém todo transforma as cargas úteis e as propostas apoiadas pelo cliente - Payload das trocas de chave - Iniciador ID da fase 1 - Nonce
	50411:28:30.30408/24/12Sev=Info/4IKE/0x63000013 ENVIANDO ISAKMP OAK AG do >>> (SA, KE, NON, ID, VID(Xauth), VID(dpd), VID(Frag), VID (NAT-T), VID(Unity)) a 64.102.156.88		Envie AM1.
	========== agressivo da mensagem 1 do <========== (AM1)		
Receba AM1 do cliente.	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEBERAM a mensagem (msgid=0) com cargas úteis: HDR + SA (1) + KE (4) +	50611:28:30.33308/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_WAIT_MSG2Event: EV_NO_EVENT	Espera para a resposta do server.

	NONCE (10) + ID (5) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NENHUNS (0) comprimentos total: 849		

Processo AM1. Compare recebeu propostas e transforma-as com as aquelas já configuradas para fósforos.
Configuração relevante:
O ISAKMP é permitido na relação, e pelo menos uma política é definida que combina o 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 túneis que combina o presente do nome da identidade:
`tunnel-group EZ type remote-access`
`tunnel-group EZ general-attributes`
`default-group-policy EZ`
`tunnel-group EZ ipsec-attributes`
`pre-shared-key cisco`
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, processando o payload SA
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, processando o payload KE
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, processando o payload ISA_KE
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, processando o payload do nonce
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, payload do processamento ID
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, processando o payload VID
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, o Xauth recebido V6 VID
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, processando o payload VID
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, DPD recebido VID
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, processando o payload VID
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, a fragmentação recebida VID
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, par IKE incluíram bandeiras da capacidade da fragmentação IKE: Modo principal: Modo de TrueAggressive: Falso
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, processando o payload VID
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, o ver recebido 02 VID de NAT-Traversal
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, processando o payload VID
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] IP= 64.102.156.87, o cliente recebido VID do Cisco Unity
	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, conexão aterrada no IPsec do tunnel_group
	24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o	

	IPsec, IP= 64.102.156.87, processando o payload IKE SA 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto falha de 11:31:03 [IKEv1]Phase 1: Tipos combinados mal do atributo para a descrição do grupo da classe: Rcv'd: Grupo 2Cfg'd: Grupo 5 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, proposta IKE SA # 1, transformam # 5 entrada global dos	

	acceptableMatches IKE # 1	
Construção AM2. Este processo inclui: - políticas escolhidas - Diffie-Hellman (DH) - Que responde ID - AUTH - Payload da detecção do Network Address Translation (NAT)	24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload ISAKMP SA 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload KE 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload do nonce 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, gerando chaves para o que responde… 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload ID 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload da mistura 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, computando a mistura para o ISAKMP 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload do Cisco Unity VID 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload do Xauth V6 VID 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload do vid do dpd 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload do ver 02 de NAT-Traversal VID 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload da NAT-descoberta 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, computando a mistura da descoberta NAT 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload da NAT-descoberta 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, computando a mistura da descoberta NAT 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo a fragmentação VID + estenderam o payload das capacidades 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload VID 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, enviam Altiga/Cisco VPN3000/Cisco ASA GW VID	
Envie AM2.	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87,	

	IKE_DECODE que ENVIA a mensagem (msgid=0) com cargas úteis: HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + MISTURA (8) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + VENDEDOR (13) + NAT-D (130) + NAT-D (130) + VENDEDOR (13) + VENDEDOR (13) + NENHUNS (0) comprimentos total: 444	
	==========> agressivo da mensagem 2 do ========== (AM2)	
	50711:28:30.40208/24/12Sev=Info/5IKE/0x6300002F Pacote ISAKMP recebido: par = 64.102.156.8 50811:28:30.40308/24/12Sev=Info/4IKE/0x63000014 RECEBENDO ISAKMP OAK AG do <<< (SA, KE, NON, ID, MISTURA, VID(Unity), VID(Xauth), VID(dpd), VID (NAT-T), NAT-D, NAT-D, VID(Frag), VID (?)) de 64.102.156.88 51011:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_RCVD_MSG	Receba AM2.
	51111:28:30.41208/24/12Sev=Info/5IKE/0x63000001 O par é um par complacente do Cisco Unity 51211:28:30.41208/24/12Sev=Info/5IKE/0x63000001 O par apoia o XAUTH 51311:28:30.41208/24/12Sev=Info/5IKE/0x63000001 O par apoia o DPD 51411:28:30.41208/24/12Sev=Info/5IKE/0x63000001 O par apoia o NAT-T 51511:28:30.41208/24/12Sev=Info/5IKE/0x63000001 O par apoia cargas úteis da fragmentação IKE 51611:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_GEN_SKEYID 51711:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_AUTHENTICATE_PEER 51811:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_ADJUST_PORT 51911:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_CRYPTO_ACTIVE	Processo AM 2.
	52011:28:30.42208/24/12Sev=Debug/7IKE/0x63000076	Construção AM3. Este processo

	NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Event: EV_BLD_MSG] 52111:28:30.42208/24/12Sev=Debug/8IKE/0x63000001 O Vendor ID Contruction IO começou 52211:28:30.42208/24/12Sev=Info/6IKE/0x63000001 Vendor ID Contruction IO bem sucedido	inclui o AUTH do cliente. Todos os dados relevantes para a criptografia têm sido trocados neste momento já.
	52311:28:30.42308/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Event: EV_SND_MSG 52411:28:30.42308/24/12Sev=Info/4IKE/0x63000013 ENVIANDO ISAKMP OAK AG DO >>> * (A MISTURA, NOTIFICA: STATUS_INITIAL_CONTACT, NAT-D, NAT-D, VID (?), VID(Unity)) a 64.102.156.88	Envie AM3.
	========== agressivo da mensagem 3 do <========== (AM3)	
Receba AM3 do cliente.	24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEBERAM a mensagem (msgid=0) com cargas úteis: HDR + a MISTURA (8) + NOTIFICAM (11) + NAT-D (130) + NAT-D (130) + o VENDEDOR (13) + o VENDEDOR (13) + NENHUNS (0) comprimentos total: 168	
O processo AM 3. confirma o uso do traversal NAT (NAT-T). Os ambos os lados estão agora prontos para começar a criptografia de tráfego.	24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, processando o payload da mistura 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, computando a mistura para o ISAKMP 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, processando notificam o payload 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, processando o payload da NAT-descoberta 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, computando a mistura da descoberta NAT 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, processando o payload da NAT-descoberta 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, computando a mistura da descoberta NAT 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, processando o payload VID 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, processando o payload do Vendor ID IOS/PIX (versão: 1.0.0, capacidades: 00000408) 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o	

	IPsec, IP= 64.102.156.87, processando o payload VID 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, receberam o cliente VID do Cisco Unity 24 de agosto 11:31:03 [IKEv1]Group = IPsec, IP= 64.102.156.87, detecção automática NAT Status: O endISbehind remoto um deviceThisend NAT não é atrás de um dispositivo NAT	
Fase iniciada 1.5 (XAUTH), e credenciais do usuário do pedido.	24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload vazio da mistura 24 de agosto 11:31:03 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, construindo o payload da mistura do qm 24 de agosto 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE que ENVIA a mensagem (msgid=fb709d4d) com cargas úteis: HDR + MISTURA (8) + ATTR (14) + NENHUNS (0) comprimentos total: 72	
	Xauth do ========== - ==========> do pedido das credenciais	
	53511:28:30.43008/24/12Sev=Info/4IKE/0x63000014 RECEBENDO O transporte do ISAKMP OAK do <<< * (MISTURA, ATTR) de 64.102.156.88 53611:28:30.43108/24/12Sev=Decode/11IKE/0x63000001 Encabeçamento ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Que responde COOKIE:1B301D2DE710EDA0 Payload seguinte: Mistura Ver (Hex):10 Tipo da troca: Transação Bandeiras: (Criptografia) MessageID(Hex):FB709D4D Length:76 Mistura do payload Payload seguinte: Atributos Reservado: 00 Comprimento de carga útil: 24 Dados (em encantar): C779D5CBC5C75E3576C478A15A7CAB8A83A232D0 Atributos do payload Payload seguinte: Nenhum Reservado: 00 Comprimento de carga útil: 20 Digite: ISAKMP_CFG_REQUEST Reservado: 00 Identificador: 0000 Tipo do XAUTH: Genérico Nome de usuário do XAUTH: (vazio) Senha do usuário do XAUTH: (vazio) 53711:28:30.43108/24/12Sev=Debug/7IKE/0x63000076	Receba a solicitação de autorização. As mostras decifradas do payload esvaziam campos do nome de usuário e senha.

	NAV Trace->TM:MsgID=FB709D4DCurState: TM_INITIALEvent: EV_RCVD_MSG	
	53811:28:30.43108/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent: EV_INIT_XAUTH 53911:28:30.43108/24/12 Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent: EV_START_RETRY_TMR 54011:28:30.43208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_NO_EVENT 541 11:28:36.41508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_RCVD_USER_INPUT	Fase iniciada 1.5 (XAUTH). Temporizador iniciado da nova tentativa como espera a entrada de usuário. Quando o temporizador da nova tentativa é executado para fora, a conexão está desligada automaticamente.
	54211:28:36.41508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_SND_MSG 54311:28:36.41508/24/12Sev=Info/4IKE/0x63000013 ENVIANDO O transporte do ISAKMP OAK do >>> * (MISTURA, ATTR) a 64.102.156.88 54411:28:36.41508/24/12Sev=Decode/11IKE/0x63000001 Encabeçamento ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Que responde COOKIE:1B301D2DE710EDA0 Payload seguinte: Mistura Ver (Hex):10 Tipo da troca: Transação Bandeiras: (Criptografia) MessageID(Hex):FB709D4D Length:85 Mistura do payload Payload seguinte: Atributos Reservado: 00 Comprimento de carga útil: 24 Dados (em encantar): 1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5 Atributos do payload Payload seguinte: Nenhum Reservado: 00 Comprimento de carga útil: 33 Digite: ISAKMP_CFG_REPLY Reservado: 00 Identificador: 0000 Tipo do XAUTH: Genérico Nome de usuário do XAUTH: (dados não indicados) Senha do usuário do XAUTH: (dados não indicados)	Uma vez que a entrada de usuário é recebida, envie credenciais do usuário ao server. As mostras decifradas do payload encheram (mas hidden) campos do nome de usuário e senha. Envie o pedido do config de modo (vários atributos).

	Xauth do <========== - ========== das credenciais do usuário	
Receba credenciais do usuário.	24 de agosto 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEBERAM a mensagem (msgid=fb709d4d) com cargas úteis: HDR + MISTURA (8) + ATTR (14) + NENHUNS (0) comprimento total: 85 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, process_attr(): Entre!	
Processe credenciais do usuário. Verifique credenciais, e gerencia o payload do config de modo. Configuração relevante: `username cisco password cisco`	24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, IP= 64.102.156.87, processando atributos da resposta MODE_CFG. 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, IKEGetUserAttributes: DN principais = 192.168.1.99 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, IKEGetUserAttributes: DN secundários = cancelado 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, IKEGetUserAttributes: VITÓRIAS preliminares = cancelado 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, IKEGetUserAttributes: VITÓRIAS secundárias = cancelado 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, IKEGetUserAttributes: lista = separação do Split Tunneling 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, IKEGetUserAttributes: domínio padrão = jyoungta-labdomain.cisco.com 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, IKEGetUserAttributes: A compressão IP = desabilitou 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, IKEGetUserAttributes: A política do Split Tunneling = desabilitou 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, IKEGetUserAttributes: O ajustes do proxy do navegador = nenhum-altera 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, IKEGetUserAttributes: Local = desabilitação do desvio do proxy do navegador 24 de agosto 11:31:09 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, usuário (usuário1) autenticado.	
Envie o resultado do	24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o	

xuath.	IPsec, username = usuário1, IP= 64.102.156.87, construindo o payload vazio da mistura 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, construindo o payload da mistura do qm 24 de agosto 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE que ENVIA a mensagem (msgid=5b6910ff) com cargas úteis: HDR + MISTURA (8) + ATTR (14) + NENHUNS (0) comprimentos total: 64	
	Xauth do ========== - ==========> do resultado da autorização	
	54511:28:36.41608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_XAUTHREQ_DONE 54611:28:36.41608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_NO_EVENT 54711:28:36.42408/24/12Sev=Info/5IKE/0x6300002F Pacote ISAKMP recebido: par = 64.102.156.88 54811:28:36.42408/24/12Sev=Info/4IKE/0x63000014 RECEBENDO O transporte do ISAKMP OAK do <<< * (MISTURA, ATTR) de 64.102.156.88 54911:28:36.42508/24/12Sev=Decode/11IKE/0x63000001 Encabeçamento ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Que responde COOKIE:1B301D2DE710EDA0 Payload seguinte: Mistura Ver (Hex):10 Tipo da troca: Transação Bandeiras: (Criptografia) MessageID(Hex):5B6910FF Length:76 Mistura do payload Payload seguinte: Atributos Reservado: 00 Comprimento de carga útil: 24 Dados (em encantar): 7DCF47827164198731639BFB7595F694C9DDFE85 Atributos do payload Payload seguinte: Nenhum Reservado: 00 Comprimento de carga útil: 12 Digite: ISAKMP_CFG_SET Reservado: 00 Identificador: 0000 Estado do XAUTH: Aprovado 55011:28:36.42508/24/12Sev=Debug/7IKE/0x63000076	Receba resultados do AUTH, e resultados do processo.

	NAV Trace->TM:MsgID=5B6910FFCurState: TM_INITIALEvent: EV_RCVD_MSG 55111:28:36.42508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_INIT_XAUTH 55211:28:36.42508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_CHK_AUTH_RESULT	
	55311:28:36.42508/24/12Sev=Info/4IKE/0x63000013 ENVIANDO O transporte do ISAKMP OAK do >>> * (MISTURA, ATTR) a 64.102.156.88	Resultado ACK.
	Xauth do <========== - ========== do reconhecimento	
Receba e processe o ACK; nenhuma resposta do server.	24 de agosto 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEBERAM a mensagem (msgid=5b6910ff) com cargas úteis: HDR + MISTURA (8) + ATTR (14) + NENHUNS (0) comprimentos total: 60 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, process_attr(): Entre! 24 de agosto 11:31:09 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, processando atributos do cfg ACK	
	55511:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_XAUTH_DONE_SUC 55611:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_NO_EVENT 55711:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_TERM_REQUEST 55811:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_REMOVE 55911:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_NO_EVENT 56011:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_XAUTH_PROGEvent: EV_XAUTH_DONE_SUC	Gerencia o pedido do config de modo. As mostras decifradas do payload pediram parâmetros do server.

	56111:28:38.40608/24/12Sev=Debug/8IKE/0x6300004C Começando o temporizador DPD para IKE SA (I_Cookie=D56197780D7BE3E5) Sa->state R_Cookie=1B301D2DE710EDA0 = 1, sa->dpd.worry_freq(mSec) = 5000 56211:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_MODECFG 56311:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_NO_EVENT 56411:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_INITIALEvent: EV_INIT_MODECFG 56511:28:38.40808/24/12Sev=Info/5IKE/0x6300005E Cliente que envia um pedido do Firewall ao concentrador 56611:28:38.40908/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_START_RETRY_TMR	
	56711:28:38.40908/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_SND_MSG 56811:28:38.40908/24/12Sev=Info/4IKE/0x63000013 ENVIANDO O transporte do ISAKMP OAK do >>> * (MISTURA, ATTR) a 64.102.156.88 56911:28:38.62708/24/12Sev=Decode/11IKE/0x63000001 Encabeçamento ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Que responde COOKIE:1B301D2DE710EDA0 Payload seguinte: Mistura Ver (Hex):10 Tipo da troca: Transação Bandeiras: (Criptografia) MessageID(Hex):84B4B653 Length:183 Mistura do payload Payload seguinte: Atributos Reservado: 00 Comprimento de carga útil: 24 Dados (em encantar): 81BFBF6721A744A815D69A315EF4AAA571D6B687	Envie o pedido do config de modo.

	Atributos do payload Payload seguinte: Nenhum Reservado: 00 Comprimento de carga útil: 131 Digite: ISAKMP_CFG_REQUEST Reservado: 00 Identificador: 0000 Endereço do IPv4: (vazio) Máscara de rede do IPv4: (vazio) IPv4 DNS: (vazio) IPv4 NBNS (VITÓRIAS): (vazio) Expiração do endereço: (vazio) Extensão Cisco: Bandeira: (vazio) Extensão Cisco: Salvar o PWD: (vazio) Extensão Cisco: Domain Name do padrão: (vazio) Extensão Cisco: A separação inclui: (vazio) Extensão Cisco: Nome do DNS em divisão: (vazio) Extensão Cisco: Faça o PFS: (vazio) Desconhecido: (vazio) Extensão Cisco: Servidores de backup: (vazio) Extensão Cisco: Disconexão da remoção da placa inteligente: (vazio) Versão de aplicativo: Cisco Systems VPN client 5.0.07.0290:WinNT Extensão Cisco: Tipo do Firewall: (vazio) Extensão Cisco: Hostname dos DN Dinâmicos: ATBASU-LABBOX		
	========== do pedido do config de modo do <==========		
Receba o pedido do config de modo.	24 de agosto 11:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEBEU a mensagem (msgid=84b4b653) com cargas úteis: HDR + MISTURA (8) + ATTR (14) + NENHUNS (0) comprimentos total: 183 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec,	57011:28:38.62808/24/12Sev= Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_NO_EVENT	Espera para a resposta de servidor.

	username = usuário1, IP= 64.102.156.87, process_attr(): Entre!		
Pedido do config de modo do processo. Muitos destes valores são configurados geralmente na grupo-política. Contudo, desde que o server neste exemplo tem muito uma configuração básica, você não os vê aqui.	24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, processando atributos do pedido do cfg 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para o endereço IPV4! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para o disfarce de rede IPV4! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para o endereço de servidor de DNS! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para o endereço do servidor das VITÓRIAS! 24 de agosto 11:31:11 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, atributo unsupported recebido do modo de transação: 5 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para a bandeira! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para o ajuste picowatt da salvaguarda! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para o Domain Name do padrão! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para a lista do túnel em divisão! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para o DNS em divisão! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para o ajuste PFS! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para o ajustes do proxy do navegador cliente! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87,	

	MODE_CFG: Pedido recebido para a lista de peer IP-SEC alternativa! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: O pedido recebido para a remoção de Smartcard do cliente desliga o ajuste! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para a versão de aplicativo! 24 de agosto 11:31:11 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, tipo de cliente: Versão de aplicativo de WinNTClient: 5.0.07.0290 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: Pedido recebido para FWTYPE! 24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, MODE_CFG: O pedido recebido para o hostname DHCP para o DDNS é: ATBASU-LABBOX!	

Construa a resposta do config de modo com todos os valores que são configurados.
Configuração relevante:
Note neste caso, o usuário é atribuído sempre 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 enableddns-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 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, obtiveram o ADDR IP (192.168.1.100) antes de iniciar o modo Cfg (o Xauth permitido)
	24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, enviando a máscara de sub-rede (255.255.255.0) ao cliente remoto
	24 de agosto 11:31:11 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, atribuíram o endereço IP privado 192.168.1.100 ao usuário remoto
	24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, construindo o payload vazio da mistura
	24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, construct_cfg_set: domínio padrão = jyoungta-labdomain.cisco.com
	24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, enviam atributos do proxy do navegador cliente!
	24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, proxy do navegador ajustado Nenhum-para alterar. Os dados do proxy do navegador não serão incluídos na resposta MODE-CFG
	24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, enviam a disconexão da remoção de Cisco Smartcard permitem!!
	24 de agosto 11:31:11 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87,	

	construindo o payload da mistura do qm		
Envie a resposta do config de modo.	24 de agosto 11:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE que ENVIA a mensagem (msgid=84b4b653) com cargas úteis: HDR + MISTURA (8) + ATTR (14) + NENHUNS (0) comprimentos total: 215		
	==========> da resposta do config de modo do ==========		
	57111:28:38.63808/24/12Sev=Info/5IKE/0x6300002F Pacote ISAKMP recebido: par = 64.102.156.88 57211:28:38.63808/24/12Sev=Info/4IKE/0x63000014 RECEBENDO O transporte do ISAKMP OAK do <<< * (MISTURA, ATTR) de 64.102.156.88 57311:28:38.63908/24/12Sev=Decode/11IKE/0x63000001 Encabeçamento ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Que responde COOKIE:1B301D2DE710EDA0 Payload seguinte: Mistura Ver (Hex):10 Tipo da troca: Transação Bandeiras: (Criptografia) MessageID(Hex):84B4B653 Length:220 Mistura do payload Payload seguinte: Atributos Reservado: 00 Comprimento de carga útil: 24 Dados (em encantar): 6DE2E70ACF6B1858846BC62E590C00A66745D14D Atributos do payload Payload seguinte: Nenhum Reservado: 00 Comprimento de carga útil: 163 Digite: ISAKMP_CFG_REPLY Reservado: 00 Identificador: 0000 Endereço do IPv4: 192.168.1.100 Máscara de rede do IPv4: 255.255.255.0 IPv4 DNS: 192.168.1.99 Extensão Cisco: Salvar o PWD: Não Extensão Cisco: Domain Name do padrão: jyoungta-labdomain.cisco.com Extensão Cisco: Faça o PFS: Não Versão de aplicativo: Cisco Systems, versão 8.4(4)1 Inc ASA5505 construída por construtores em Thu 14-Jun-12 11:20 Extensão Cisco: Disconexão da remoção da placa inteligente: Sim		Receba valores de parâmetro do config de modo do server.
A fase 1 termina no server. Processo iniciado do quick mode (QM).	24 de agosto 11:31:13 [IKEv1 DESCODIFIC	57411:28:38.63908/24/12Sev= Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState:	Os parâmetros de processo, e configuram-se em

	AM] IP= 64.102.156.87, que responde IKE que começa o QM: msg identificação = 0e83792e 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, Quick Mode do atraso que processa, CERT/transporte Exch/RM DSID em andamento 24 de agosto 11:31:13 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, ARP gratuito enviado para 192.168.1.100 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, Quick Mode do resumo que processa, CERT/transporte Exch/RM DSID terminado 24 de agosto 11:31:13 [IKEv1]Group	TM_WAIT_MODECFGREPLYEvent: EV_RCVD_MSG 57511:28:38.63908/24/12Sev= Info/5IKE/0x63000010 MODE_CFG_REPLY: Atributo = INTERNAL_IPV4_ADDRESS: , valor = 192.168.1.100 57611:28:38.63908/24/12Sev=Info/5IKE/0x63000010 MODE_CFG_REPLY: Atributo = INTERNAL_IPV4_NETMASK: , valor = 255.255.255.0 57711:28:38.63908/24/12Sev= Info/5IKE/0x63000010 MODE_CFG_REPLY: Atributo = INTERNAL_IPV4_DNS(1): , valor = 192.168.1.99 57811:28:38.63908/24/12Sev=Info/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = MODECFG_UNITY_SAVEPWD: , valor = 0x00000000 57911:28:38.63908/24/12Sev=Info/5IKE/0x6300000E MODE_CFG_REPLY: Atributo = MODECFG_UNITY_DEFDOMAIN: , valor = jyoungta-labdomain.cisco.com 58011:28:38.63908/24/12Sev= Info/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = MODECFG_UNITY_PFS: , valor = 0x00000000 58111:28:38.63908/24/12Sev=Info/5IKE/0x6300000E MODE_CFG_REPLY: Atributo = APPLICATION_VERSION, valor = Cisco Systems, versão 8.4(4)1 Inc ASA5505 construída por construtores em Thu 14-Jun-12 11:20 58211:28:38.63908/24/12Sev= Info/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = MODECFG_UNITY_SMARTCARD_REMOVAL_DISCONNECT: , valor = 0x00000001 58311:28:38.63908/24/12Sev= Info/5IKE/0x6300000D MODE_CFG_REPLY: Atributo = recebido e usando o NAT-T número de porta, valor = 0x00001194 58411:28:39.36708/24/12Sev= Debug/9IKE/0x63000093	conformidade.

	= IPsec, username = usuário1, IP= 64.102.156.87, FASE 1 TERMINADA	O valor para o parâmetro ini EnableDNSRedirection é 1 58511:28:39.36708/24/12Sev= Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_MODECFG_DONEEvent: EV_MODECFG_DONE_SUC	
Construa e envie o DPD para o cliente.	24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, tipo da manutenção de atividade para esta conexão: DPD 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, começando o P1 rekey o temporizador: 82080 segundos. 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, enviando notificam a mensagem 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, construindo o payload vazio da mistura 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, construindo o payload da mistura do qm 24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE que ENVIA a mensagem (msgid=be8f7821) com cargas úteis: HDR + a MISTURA (8) + NOTIFICAM (11) + NENHUNS (0) comprimentos total: 92	
	==========> do Dead Peer Detection do ========== (DPD)		
	58811:28:39.79508/24/12Sev=Debug/7IKE/0x63000015 intf_data: lcl=0x0501A8C0, mask=0x00FFFFFF, bcast=0xFF01A8C0, bcast_vra=0xFF07070A 58911:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_P2 59011:28:39.79508/24/12Sev=Info/4IKE/0x63000056 Recebeu um pedido chave do direcionador: IP local = 192.168.1.100, GW IP= 64.102.156.88, IP remoto = 0.0.0.0 59111:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_ACTIVEEvent: EV_NO_EVENT 59211:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_INITIALEvent: EV_INITIATOR 59311:28:39.79508/24/12Sev=Debug/7IKE/0x6300007	QM iniciado, construção QM1 da fase 2. Este processo inclui: - Mistura - SA com todas as propostas da fase 2 apoiadas pelo cliente, pelo tipo de túnel e pela criptografia - Nonce - Identificação de cliente - Proxy ID

	6 NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG1Event: EV_CHK_PFS 59411:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG1Event: EV_BLD_MSG 59511:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG1Event: EV_START_RETRY_TMR	
	59611:28:39.79608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG1Event: EV_SND_MSG 59711:28:39.79608/24/12Sev=Info/4IKE/0x63000013 ENVIANDO O ISAKMP OAK QM do >>> * (MISTURA, SA, NON, ID, ID) a 64.102.156.88	Envie QM1.
	========== da mensagem 1 do Quick Mode do <========== (QM1)	
Receba QM1.	24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEBERAM a mensagem (msgid=e83792e) com cargas úteis: HDR + MISTURA (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NENHUNS (0) comprimentos total: 1026	
Processo QM1. Configuração relevante: `crypto dynamic-map DYN 10 set transform-set TRA`	24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, processando o payload da mistura 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, processando o payload SA 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, processando o payload do nonce 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, payload do processamento ID 24 de agosto 11:31:13 [IKEv1 DESCODIFICAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, ID_IPV4_ADDR ID recebido 192.168.1.100 24 de agosto 11:31:13 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, receberam dados de host remotos do proxy no payload ID: Enderece 192.168.1.100, o protocolo 0, a porta 0 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, payload do processamento ID 24 de agosto 11:31:13 [IKEv1 DESCODIFICAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, ID_IPV4_ADDR_SUBNET ID received--0.0.0.0--0.0.0.0 24 de agosto 11:31:13 [IKEv1]Group = IPsec,	

	username = usuário1, IP= 64.102.156.87, receberam dados da sub-rede do proxy do IP local no payload ID: Enderece 0.0.0.0, máscara 0.0.0.0, o protocolo 0, a porta 0 24 de agosto 11:31:13 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, sa velho QM IsRekeyed não encontrado pelo ADDR 24 de agosto 11:31:13 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, verificação do mapa estático de criptografia, verificando o mapa = o para fora-mapa, segs.s = 10… 24 de agosto 11:31:13 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, verificação do mapa estático de criptografia contorneada: Entrada do crypto map incompleta! 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, selecionando somente os modos do andUDP-Encapsular-transporte do UDP-Encapsular-túnel definidos por NAT-Traversal 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, selecionando somente os modos do andUDP-Encapsular-transporte do UDP-Encapsular-túnel definidos por NAT-Traversal 24 de agosto 11:31:13 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, peer remoto IKE configurado para o crypto map: para fora-dyn-mapa 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, processando o payload IPsec SA	

Construção 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`
	24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, proposta IPsec SA # 12, transformam # 1 entrada IPsec SA dos acceptableMatches # 10 globais
	24 de agosto 11:31:13 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, IKE: pedindo o SPI!
	IPSEC: @ 0xcfdffc90 criado SA embrionário novo, SCB: 0xCFDFFB58, sentido: de entrada
	SPI: 0x9E18ACB2
	ID de sessão: 0x00138000
	VPIF numérico: 0x00000004
	Tipo de túnel: ra
	Protocolo: esp
	Duração: 240 segundos
	24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, IKE obtiveram o SPI do motor chave: SPI = 0x9e18acb2
	24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, oakley que constrói o Quick Mode	

DYN crypto map MAP interface outside	24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, construindo o payload vazio da mistura 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, construindo o payload IPsec SA 24 de agosto 11:31:13 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, o IPsec do iniciador da ultrapassagem que rekeying a duração de 2147483 a 86400 segundos 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, construindo o payload do nonce do IPsec 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, construindo o ID de proxy 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, transmitindo a identificação do proxy: Host remoto: 192.168.1.100Protocol 0Port 0 Protocolo local 0Port 0 subnet:0.0.0.0mask 0.0.0.0 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, enviando a notificação da VIDA do QUE RESPONDE ao iniciador 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, construindo o payload da mistura do qm	
Envie QM2.	24 de agosto 11:31:13 [IKEv1 DESCODIFICAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, que responde IKE que envia o ò pkt QM: msg identificação = 0e83792e 24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE que ENVIA a mensagem (msgid=e83792e) com cargas úteis: HDR + a MISTURA (8) + SA (1) + o NONCE (10) + ID (5) + ID (5) + NOTIFICAM (11) + NENHUNS (0) comprimentos total: 184	
	==========> da mensagem 2 do Quick Mode do ========== (QM2)	
	60811:28:39.96208/24/12Sev=Info/4IKE/0x63000014 RECEBENDO O ISAKMP OAK QM DO <<< * (MISTURA, SA, NON, ID, ID, NOTIFIQUE: STATUS_RESP_LIFETIME) de 64.102.156.88	Receba QM2.
	60911:28:39.96408/24/12Sev=Decode/11IKE/0x63000001 Encabeçamento ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Que responde COOKIE:1B301D2DE710EDA0 Payload seguinte: Mistura Ver (Hex):10 Tipo da troca: Quick Mode	Processe QM2. Propostas escolhidas mostras decifradas do payload.

	Bandeiras: (Criptografia) MessageID(Hex):E83792E Length:188 Mistura do payload Payload seguinte: Associação de segurança Reservado: 00 Comprimento de carga útil: 24 Dados (em encantar): CABF38A62C9B88D1691E81F3857D6189534B2EC0 Associação de segurança do payload Payload seguinte: Nonce Reservado: 00 Comprimento de carga útil: 52 DOI: IPsec Situação: (SIT_IDENTITY_ONLY) Proposta do payload Payload seguinte: Nenhum Reservado: 00 Comprimento de carga útil: 40 Proposta #: 1 ID de protocolo: PROTO_IPSEC_ESP Tamanho SPI: 4 # de transforma: 1 SPI: 9E18ACB2 O payload transforma Payload seguinte: Nenhum Reservado: 00 Comprimento de carga útil: 28 Transforme #: 1 Transformar-identificação: ESP_3DES Reserved2: 0000 Tipo da vida: Segundos Duração da vida (encantar): 0020C49B Modo de encapsulamento: Túnel UDP Algoritmo de autenticação: SHA1 Nonce do payload Payload seguinte: Identificação Reservado: 00 Comprimento de carga útil: 24 Dados (em encantar): 3A079B75DA512473706F235EA3FCA61F1D15D4CD Identificação do payload Payload seguinte: Identificação Reservado: 00 Comprimento de carga útil: 12 Tipo ID: Endereço do IPv4 ID de protocolo (UDP/TCP, etc…): 0 Porta: 0 ID Data: 192.168.1.100 Identificação do payload Payload seguinte: Notificação	

	Reservado: 00 Comprimento de carga útil: 16 Tipo ID: Sub-rede do IPv4 ID de protocolo (UDP/TCP, etc…): 0 Porta: 0 ID Data: 0.0.0.0/0.0.0.0 Notificação do payload Payload seguinte: Nenhum Reservado: 00 Comprimento de carga útil: 28 DOI: IPsec ID de protocolo: PROTO_IPSEC_ESP Tamanho de Spi: 4 Notifique o tipo: STATUS_RESP_LIFETIME SPI: 9E18ACB2 Data: Tipo da vida: Segundos Duração da vida (encantar): 00015180	
	61011:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Event: EV_RCVD_MSG 61111:28:39.96508/24/12Sev=Info/5IKE/0x63000045 RESPONDER-LIFETIME notificam têm um valor de 86400 segundos 61211:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Event: EV_CHK_PFS 61311:28:39.96508/24/12Sev=Debug/7IKE/0x63000076	Processo QM2.
	NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG3Event: EV_BLD_MSG 61411:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 Encabeçamento ISAKMP Iniciador COOKIE:D56197780D7BE3E5 Que responde COOKIE:1B301D2DE710EDA0 Payload seguinte: Mistura Ver (Hex):10 Tipo da troca: Quick Mode Bandeiras: (Criptografia) MessageID(Hex):E83792E Length:52 Mistura do payload Payload seguinte: Nenhum Reservado: 00 Comprimento de carga útil: 24 Dados (em encantar): CDDC20D91EB4B568C826D6A5770A5CF020141236	Construa QM3. Payload decifrado para QM3 mostrado aqui. Esta mistura dos ncludes do processo.
	61511:28:39.96508/24/12Sev=Debug/7IKE/0x63000076	Envie QM3. O cliente está agora

	NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG3Event: EV_SND_MSG 61611:28:39.96508/24/12Sev=Info/4IKE/0x63000013 ENVIANDO O ISAKMP OAK QM do >>> * (MISTURA) a 64.102.156.88	pronto para cifrar e decifrar.
	========== da mensagem 3 do Quick Mode do <========== (QM3)	
Receba QM3.	24 de agosto 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEBERAM a mensagem (msgid=e83792e) com cargas úteis: HDR + MISTURA (8) + NENHUNS (0) comprimentos total: 52	

Processo QM3. Crie os deslocamentos predeterminados de entrada e de partida do parâmetro de segurança (SPI). Adicionar a 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 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, processando o payload da mistura
	24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, carregando todo o sas de IPSec
	24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, gerando a chave do Quick Mode!
	24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, NP cifram a regra olham acima para o para fora-dyn-mapa 10 do crypto map que combina o desconhecido ACL: retornado
	cs_id=cc107410; rule=00000000
	24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, gerando a chave do Quick Mode!
	IPSEC: @ 0xccc9ed60 criado SA embrionário novo, SCB: 0xCF7F59E0,
	Direção: saída
	SPI: 0xC055290A
	ID de sessão: 0x00138000
	VPIF numérico: 0x00000004
	Tipo de túnel: ra
	Protocolo: esp
	Duração: 240 segundos
	IPSEC: Atualização terminada do host OBSA, SPI 0xC055290A
	IPSEC: Criando o contexto de partida VPN, SPI 0xC055290A
	Bandeiras: 0x00000025
	SA: 0xccc9ed60
	SPI: 0xC055290A
	MTU: 1500 bytes
	VCID: 0x00000000
	Correspondente: 0x00000000
	SCB: 0xA5922B6B
	Canal: 0xc82afb60
	IPSEC: Contexto de partida terminado VPN, SPI 0xC055290A
	Punho VPN: 0x0015909c	

	IPSEC: De partida novos cifram a regra, SPI 0xC055290A ADDR de Src: 0.0.0.0 Máscara de Src: 0.0.0.0 ADDR de Dst: 192.168.1.100 Máscara de Dst: 255.255.255.255 Portas de Src Parte superior: 0 Abaixe: 0 Op: ignore Portas de Dst Parte superior: 0 Abaixe: 0 Op: ignore Protocolo: 0 Protocolo do uso: falso SPI: 0x00000000 Uso SPI: falso IPSEC: De partida terminados cifram a regra, SPI 0xC055290A Regra ID: 0xcb47a710 IPSEC: Regra de partida nova da licença, SPI 0xC055290A ADDR de Src: 64.102.156.88 Máscara de Src: 255.255.255.255 ADDR de Dst: 64.102.156.87 Máscara de Dst: 255.255.255.255 Portas de Src Parte superior: 4500 Abaixe: 4500 Op: igual Portas de Dst Parte superior: 58506 Abaixe: 58506 Op: igual Protocolo: 17 Protocolo do uso: verdadeiro SPI: 0x00000000 Uso SPI: falso IPSEC: Regra de partida terminada da licença, SPI 0xC055290A Regra ID: 0xcdf3cfa0 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, NP cifram a regra olham acima para o para fora-dyn-mapa 10 do crypto map que combina o desconhecido ACL: retornado cs_id=cc107410; rule=00000000 24 de agosto 11:31:13 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, negociação de segurança completa para o usuário (user1)Responder, de entrada SPI = 0x9e18acb2, de partida	

	SPI = 0xc055290a 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, IKE obteve um msg KEY_ADD para o SA: SPI = 0xc055290a IPSEC: Atualização terminada do host IBSA, SPI 0x9E18ACB2 IPSEC: Criando o contexto de entrada VPN, SPI 0x9E18ACB2 Bandeiras: 0x00000026 SA: 0xcfdffc90 SPI: 0x9E18ACB2 MTU: bytes 0 VCID: 0x00000000 Correspondente: 0x0015909C SCB: 0xA5672481 Canal: 0xc82afb60 IPSEC: Contexto de entrada terminado VPN, SPI 0x9E18ACB2 Punho VPN: 0x0016219c IPSEC: Atualizando o contexto de partida 0x0015909C VPN, SPI 0xC055290A Bandeiras: 0x00000025 SA: 0xccc9ed60 SPI: 0xC055290A MTU: 1500 bytes VCID: 0x00000000 Correspondente: 0x0016219C SCB: 0xA5922B6B Canal: 0xc82afb60 IPSEC: Contexto de partida terminado VPN, SPI 0xC055290A Punho VPN: 0x0015909c IPSEC: Regra interna de partida terminada, SPI 0xC055290A Regra ID: 0xcb47a710 IPSEC: Regra exterior de partida terminada SPD, SPI 0xC055290A Regra ID: 0xcdf3cfa0 IPSEC: Regra de entrada nova do fluxo do túnel, SPI 0x9E18ACB2 ADDR de Src: 192.168.1.100 Máscara de Src: 255.255.255.255 ADDR de Dst: 0.0.0.0 Máscara de Dst: 0.0.0.0 Portas de Src Parte superior: 0 Abaixe: 0 Op: ignore Portas de Dst Parte superior: 0 Abaixe: 0 Op: ignore	

	Protocolo: 0 Protocolo do uso: falso SPI: 0x00000000 Uso SPI: falso IPSEC: Regra de entrada terminada do fluxo do túnel, SPI 0x9E18ACB2 Regra ID: 0xcdf15270 IPSEC: Regra de entrada nova do decrypt, SPI 0x9E18ACB2 ADDR de Src: 64.102.156.87 Máscara de Src: 255.255.255.255 ADDR de Dst: 64.102.156.88 Máscara de Dst: 255.255.255.255 Portas de Src Parte superior: 58506 Abaixe: 58506 Op: igual Portas de Dst Parte superior: 4500 Abaixe: 4500 Op: igual Protocolo: 17 Protocolo do uso: verdadeiro SPI: 0x00000000 Uso SPI: falso IPSEC: Regra de entrada terminada do decrypt, SPI 0x9E18ACB2 Regra ID: 0xce03c2f8 IPSEC: Regra de entrada nova da licença, SPI 0x9E18ACB2 ADDR de Src: 64.102.156.87 Máscara de Src: 255.255.255.255 ADDR de Dst: 64.102.156.88 Máscara de Dst: 255.255.255.255 Portas de Src Parte superior: 58506 Abaixe: 58506 Op: igual Portas de Dst Parte superior: 4500 Abaixe: 4500 Op: igual Protocolo: 17 Protocolo do uso: verdadeiro SPI: 0x00000000 Uso SPI: falso IPSEC: Regra de entrada terminada da licença, SPI 0x9E18ACB2 Regra ID: 0xcf6f58c0 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o IPsec, username = usuário1, IP= 64.102.156.87, jarro: KEY_UPDATE recebido, spi 0x9e18acb2 24 de agosto 11:31:13 [IKEv1 DEBUGAM] o grupo = o	

	IPsec, username = usuário1, IP= 64.102.156.87, começando o P2 rekey o temporizador: 82080 segundos. 24 de agosto 11:31:13 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, adicionando a rota estática para o endereço de cliente: 192.168.1.100	
Fase 2 completa. Os ambos os lados são de criptografia e de descriptografia agora.	24 de agosto 11:31:13 [IKEv1]Group = IPsec, username = usuário1, IP= 64.102.156.87, FASE 2 TERMINADA (msgid=0e83792e)	
Para clientes da ferragem, uma mais mensagem é recebida onde o cliente envia a informação sobre se. Se você olha com cuidado, você deve encontrar o hostname do cliente ezvpn, o software que é executado no cliente, e o lugar e o nome do software	24 de agosto 11:31:13 [IKEv1]: O IP= 10.48.66.23, IKE_DECODE RECEBEU a mensagem (msgid=91facca9) com cargas úteis: HDR + a MISTURA (8) + NOTIFICAM (11) + NENHUNS (0) comprimentos total: 184 24 de agosto 11:31:13 [IKEv1 DEBUGAM]: Grupo = EZ, username = Cisco, IP= 10.48.66.23, processando o payload da mistura 24 de agosto 11:31:13 [IKEv1 DEBUGAM]: O grupo = o EZ, username = Cisco, IP= 10.48.66.23, processando notificam o payload 24 de agosto 11:31:13 [IKEv1 DESCODIFICAM]: DESCRITOR OBSOLETO - DESLOCAMENTO PREDETERMINADO 1 24 de agosto 11:31:13 [IKEv1 DESCODIFICAM]: 0000: 00000000 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 31363331 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 [IKEv1 DEBUGAM]: Grupo = EZ, username = Cisco, IP= 10.48.66.23, processando a mistura PSK 24 de agosto 11:31:13 [IKEv1]: Grupo = EZ, username = Cisco, IP= 192.168.1.100, tamanho incompatível da mistura PSK 24 de agosto 11:31:13 [IKEv1 DEBUGAM]: O grupo = o EZ, username = Cisco, IP= 10.48.66.23, verificação da mistura PSK falharam!	

Verificação do túnel

ISAKMP

A saída do comando **sh do det AIA sa do grito** 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

Desde que o Internet Control Message Protocol (ICMP) é usado para provocar o túnel, simplesmente um IPsec SA está acima. O protocolo 1 é ICMP. Note que os valores SPI diferem de esses negociados no debugam. Este é, de fato, o mesmo túnel após a fase 2 rekey.

A saída do comando **cripto sh 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 de Wikipedia no IPsec
- Troubleshooting de IPSec: Compreendendo e usando comandos debug
- Suporte Técnico e Documentação - Cisco Systems