ASA IPsec- en IKE-debugs (IKEv1 Aggressive Mode) voor probleemoplossing Technische opmerking

Inhoud

Inleiding

Dit document beschrijft de tekortkomingen van Cisco adaptieve security applicatie (ASA) wanneer zowel de agressieve modus als de pre-Shared key (PSK) worden gebruikt. De vertaling van bepaalde debug-lijnen in de configuratie wordt ook besproken. Cisco raadt u een basiskennis van IPsec en Internet Key Exchange (IKE) aan.

In dit document wordt niet gesproken over het passeren van het verkeer na de invoering van de tunnel.

kernvraagstuk

IKE en IPsec debugs zijn soms cryptisch, maar u kunt ze gebruiken om problemen met IPsec VPN-tunnelvestiging te begrijpen.

Scenario

Aggressieve modus wordt normaal gebruikt in het geval van Easy VPN (EzVPN) met software (Cisco VPN-client) en hardwareclients (Cisco ASA 5505 adaptieve security applicatie of Cisco IOS? Softwarerouters), maar alleen wanneer een vooraf gedeelde sleutel wordt gebruikt. In tegenstelling tot de hoofdmodus bestaat de agressieve modus uit drie berichten.

De debugs komen van een ASA die softwareversie 8.3.2 draait en werkt als een EzVPN-server. De EzVPN-client is een softwareclient.

Gebruikte opdrachten debug

Dit zijn de debug-opdrachten in dit document:

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

ASA-configuratie

De ASA-configuratie in dit voorbeeld moet strikt basiszijn; er worden geen externe servers gebruikt .

```
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
```

Ontbreken

Opmerking: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

Beschrijving van serverbericht	Debugs	
	4971:28:30.28908/24/12 Sev=Info/6IKE/0x630003B Proberen een verbinding tot stand te brengen met 64.102.156.88. 4981:28:30.29708/24/12 Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_INITIALEvent: EV_INITIATOR 4911:28:30.29708/24/12.Sev=Info/4IKE/0x6300001 IKE fase 1-onderhandeling starten 5001:28:30.29708/24/12 Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: Event en AM_SND_MSG1Event: EV_GEN_DHKEY 5011:28:30.30408/24/12008:12-Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: Event en AM_SND_MSG1Event: EV_BLD_MSG 5021:28:30.30408/24/12008:2012 Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: Event en AM_SND_MSG1Event: EV_START_RETRY_TMR 5031:28:30.30408/24/12008:12-Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: Event en AM_SND_MSG1Event: EV_SND_MSG	
	5041:28:30.30408/24/12008=Info/4IKE/0x6300013 VERZENDING >> ISAKMP OAK AG (SA, KE, NON, ID, VID(Xauth), VID(dpd) VID(Frag), VID(NAT-T), VID(Unity)) tot 64.102.156.88	
	<==========="="Aggressief bericht 1" (AM1) ==========="======"="="=")	
Ontvang AM1 van de cliënt.	24 aug. 24:31:03 [IKEv1]IP = 64.102.156.87, ONTVANGEN IKE_DECODE Bericht (msgid=0) met payload: HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR	50611:28:30.3308/24/12008:12-Sev=Debug/7IKE/0x6300076 NAV Trace-9>SA:I_Cookie=D5619780D7BE3E5 R_Cookie=0000000000000000CurState: AM_WAIT_MSG2Event: EV_NO_EVENT

	(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) totale lengte : 849	

Vergelijk ontvangen voorstellen en vergelijk ze met die welke al voor wedstrijden zijn geconfigureerd.
Relevante configuratie:
ISAKMP is ingeschakeld op interface en minstens één beleid wordt gedefinieerd dat overeenkomt met wat de klant heeft verstuurd:
 	
`crypto isakmp enable outside`
`crypto isakmp policy 10`
`authentication pre-share`
`encryption aes`
`hash sha`
`group 2`
`lifetime 86400`
Tunnelgroepen die overeenkomen met de aanwezige identificatienaam:
 	
`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 aug. 24:11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, verwerkt SA-lading
	24 aug. 24:11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, verwerking van zwar lading
	24 aug. 24:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, bewerking ISA_KE payload
	24 aug. 24:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, verwerking eenmalig
	24 aug. 24:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, payload-ID
	24 aug. 24:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, verwerking van VID-lading
	24 aug. 24:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, ontvangen behalve V6 VID
	24 aug. 24:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, verwerking van VID-lading
	24 aug. 24:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, ontvangen DPD VID
	24 aug. 24:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, verwerking van VID-lading
	24 aug. 24:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, ontvangen fragmentatie VID
	24 aug. 24:11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, bevat IKE-peer vlaggen met fragmentatievermogen: Belangrijkste modus: TrueAggressive Mode:FALSE
	24 aug. 24:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, verwerking van VID-lading
	24 aug. 24:11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, ontvangen NAT-traversal ver 02 VID
	24 aug. 24:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, verwerking van VID-lading
	24 aug. 24:11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, ontvangen Cisco Uni client-VID
	24 aug. 24:31:03 [IKEv1]IP = 64.102.156.87, verbinding landd op tunnel_grou ipsec
	24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, verwerkt IKE SA-lading
	24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5
	24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5
	24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5
	24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5
	24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5
	24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5	

	24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5 24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5 24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5 24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5 24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5 24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5 24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5 24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5 24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5 24 aug. 11:31:03 [IKEv1]Fase 1-storing:Niet-afgesloten attribuuttypes voor klasse groepbeschrijving:Rcv'd: Groep 2Cfg'd: Groep 5 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, IKE S voorstel # 1, Transformeer # 5 acceptabeleOvereenkomsten wereldwijde IKE- ingang # 1
Projectie AM2. Dit proces omvat: - gekozen beleid - Diffie-Hellman (DH) - Nummerherkenning - oostenrijk - nuttige lading voor detectie van netwerkadresomzetting (NAT)	24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, construerend ISAKMP SA-lading 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, waarb de nuttige lading wordt geconstrueerd 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, bouw eenmalig lading 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, genererende toetsen voor Responder... 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, waarb de ID-lading wordt geconstrueerd 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, voor het construeren van lading 24 aug. 24:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, Computir haash voor ISAKMP 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, waarb Cisco Unity VID-payload wordt geconstrueerd 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, waarb de maximale V6 VID-lading wordt geconstrueerd 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, waarb dpd vid-lading wordt geconstrueerd 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, waarb NAT-traversal VID wordt geconstrueerd voor 02 lading 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, voor het construeren van de lading NAT-ontdekking 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, reken NAT Discovery Hash 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, voor het construeren van de lading NAT-ontdekking 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, reken NAT Discovery Hash

	24 aug. 24:11:31:03 [IKEv1 DEBUG]Groep = ipsec, IP = 64.102.156.87, waarl de fragmentatie VID + uitgebreide mogelijkheden voor payload worden geconstrueerd 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, waarb VID-lading wordt geconstrueerd 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, Verzend Altiga/Cisco VPN3000/Cisco ASA GW VID
Stuur AM2.	24 aug. 24:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE- VERZENDingsbericht (msgid=0) met payload: HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (13) + VENDO (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + VENDOR (1 3) + VENDOR (13) + NONE (0) totale lengte : 444
	==========="="Aggressief bericht 2" (AM2) ==========="="
	5071:28:30.40208/24/12002SV=Info/5IKE/0x630002F Ontvangen ISAKMP-pakket: peer = 64.102.156,8 50811:28:30.40308/24/12008=Info/4IKE/0x6300014 ONTVANGEN < < ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID(Unity), VID(Xauth), VID(dpd), VID(NAT-T), NAT-D, NAT-D, VID(Frag), VID(?)) vanaf 64.102.156.8 88 5101:28:30.41208/24/120076:12-Sev=Debug/7IKE/0x6300076 NAV Trace-9>SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_RCVD_MSG
	5111:28:30.41208/24/120001 SV=Info/5IKE/0x6300001 Peer is een peer die compatibel is met Cisco Unity 512:11:28:30.41208/24/120001 SV=Info/5IKE/0x6300001 Peer ondersteunt XAUTH 5131:28:30.41208/24/120001 SV=Info/5IKE/0x6300001 Peer-ondersteuning DPD 1541:28:30.41208/24/120012000000000000000000000000 Peer-ondersteuning voor NAT-T 515:11:28:30.41208/24/120001 SV=Info/5IKE/0x6300001 Peer ondersteunt IKE-fragmentatie 516:11:28:30.41208/24/12008:2012 Sev=Debug/7IKE/0x6300076 NAV Trace-9>SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_GEN_SKEYID 5171:28:30.4208/24/12 Sev=Debug/7IKE/0x6300076 NAV Trace-9>SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_AUTHENTICATE_PEER 5181:28:30.4208/24/120076:12-Sev=Debug/7IKE/0x6300076 NAV Trace-9>SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_ADJUST_PORT 5191:28:30.4208/24/120076:12-Sev=Debug/7IKE/0x6300076 NAV Trace-9>SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_CRYPTO_ACTIVE
	5201:28:30.4208/24/12008:2011:28:28:30.2208/24/12012:2011:28:00 NAV Trace-9>SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Event: EV_BLD_MSG]

	5211:28:30.4208/24/12001 Sev=Debug/8IKE/0x6300001 IOS-verkoper-id: configuratie gestart 5211:28:30.4208/24/120001 SV=Info/6IKE/0x6300001 IOS-verkoper-id: succesvol
	5231:28:30.42308/24/12 Sev=Debug/7IKE/0x6300076 NAV Trace-9>SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Event: EV_SND_MSG 5241:28:30.42308/24/120013 SV=Info/4IKE/0x6300013 VERZENDING >> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT, NAT-D, NAT-D, VID(?), VID(Unity)) to 64.102.156.88
	<==========="="Aggressief bericht 3" (AM3) ==========="======"="="=")
Ontvang AM3 van client.	24 aug. 24:31:03 [IKEv1]IP = 64.102.156.87, ONTVANGEN IKE_DECODE Bericht (msgid=0) met payload: HDR + HASH (8) + MEDEDELING (11) + NAT D (130) + NAT-D (130) + VENDOR (13) + VENDOR (13) + NONE (0) totale lengte : 168
ProcesAM 3. Bevestig NAT-verkeer (NAT-T). Beide kanten zijn nu klaar om verkeersencryptie te starten.	24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, verwerkingshash payload-belasting 24 aug. 24:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, Computin haash voor ISAKMP 24 aug. 24:11:31:03 [IKEv1 DEBUG]Groep = ipsec, IP = 64.102.156.87, verwerkingskennisgeving voor payload 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, verwerking van payload-encryptie met NAT-ontdekking 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, reken NAT Discovery Hash 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, verwerking van payload-encryptie met NAT-ontdekking 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, reken NAT Discovery Hash 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, verwerking van VID-lading 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, verwerkings IOS/PIX-verkoper ID payload (versie: 1.0.0. capaciteiten: 00000408) 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, verwerking van VID-lading 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, Ontvangen Cisco Unity client-VID 24 aug. 24:11:31:03 [IKEv1]groep = ipsec, IP = 64.102.156.87, automatische NAT-detectie Status:Remote EndIS achter een NAT-apparaatDit eindpunt zit NIET achter ee NAT-apparaat
Start fase 1.5 (XAUTH) en open gebruikersreferenties.	24 aug. 24:11:31:03 [IKEv1 DEBUG]Groep = ipsec, IP = 64.102.156.87, voor het construeren van een lege hash payload-lading 24 aug. 24:11:31:03 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, construerend qm hash payload-lading 24 aug. 24:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE- VERZENDingsbericht (msgid=fb709d4d) met payload: HDR + HASH (8) + ATTR (14) + NONE (0) totale lengte: 72

	==========">Kredietinstellingen Aanvragen ==========="="="="="="">Kredietinstellingen
	5351:28:30.4308/24/12008=Info/4IKE/0x6300014 ONTVANGEN << ISAKMP OAK TRANS *(HASH, ATTR) vanaf 64.102.156.88 5361:28:30.43108/24/12 Sev=Decode/11IKE/0x6300001 ISAKMP-header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Volgende payload:slaan Ver (Hex):10 Exchange type:transactie Vlaggen:(Encryptie) Bericht (ID (Hex):FB709D4D Lengte:76 payload-hash Volgende payload: Kenmerken Voorbehouden: 00 Lengte payload: 24 Gegevens (in hex): C779D5CBC5C75E3576C478A15A7CAB8A83A232D0 payload-kenmerken Volgende payload: None Voorbehouden: 00 Lengte payload: 20 Type: ISAKMP_CFG_REQUEST Voorbehouden: 00 Identificatiecode: 0000 XAUTH-type: generiek XAUTH-gebruikersnaam: (leeg) XAUTH-gebruikerswachtwoord: (leeg) 5371:28:30.43108/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=FB709D4DCurState: TM_INITIALEvent: EV_RCVD_MSG
	5381:28:30.43108/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent EV_INIT_XAUTH 5391:28:30.43108/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent EV_START_RETRY_TMR 5401:28:30.43208/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_NO_EVENT 541 11:28:36.41508/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_RCVD_USER_INPUT
	5421:28:36.41508/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_SND_MSG 5431:28:36.41508/24/120013 SV=Info/4IKE/0x6300013 VERZENDING >> ISAKMP OAK TRANS *(HASH, ATTR) NAAR 64.102.156.8 5411:28:36.41508/24/12-Sev=Decode/11IKE/0x6300001 ISAKMP-header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0

	Volgende payload:slaan Ver (Hex):10 Exchange type:transactie Vlaggen:(Encryptie) Bericht (ID (Hex):FB709D4D Lengte:85 payload-hash Volgende payload: Kenmerken Voorbehouden: 00 Lengte payload: 24 Gegevens (in hex): 1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5 payload-kenmerken Volgende payload: None Voorbehouden: 00 Lengte payload: 33 Type: ISAKMP_CFG_REPLY Voorbehouden: 00 Identificatiecode: 0000 XAUTH-type: generiek XAUTH-gebruikersnaam: (gegevens niet weergegeven) XAUTH-gebruikerswachtwoord: (gegevens niet weergegeven)
	<=================="=" Xauth - User Credentials =================="====="="="="="="="="="="="="="="="="="="="
Ontvang gebruikersreferenties.	24 aug. 24:31:09 [IKEv1]IP = 64.102.156.87, ONTVANGEN IKE_DECODE Bericht (msgid=fb709d4d) met payload: HDR + HASH (8) + ATTR (14) + NON (0) totale lengte : 85 24 aug. 24:31:09 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, process_attr(): Kom binnen!

Gebruikershandleidingen verwerken. Controleer geloofsbrieven, en genereer mode configuratie lading. Relevante configuratie:
 	
`username cisco`
`password cisco`
	24 aug. 24:11:31:09 [IKEv1 DEBUG]groep = ipsec, IP = 64.102.156.87, attributie Processing MODE_CFG Reply.
	24 aug. 24:11:31:09 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, IKEGet UserAttributes: primaire DNS = 192.168.1.99
	24 aug. 24:11:31:09 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, IKEGet UserAttributes: secundaire DNS = gewist
	24 aug. 24:11:31:09 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, IKEGet UserAttributes: primaire WINS = geklaard
	24 aug. 24:11:31:09 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, IKEGet UserAttributes: secundaire WINS = geklaard
	24 aug. 24:11:31:09 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, IKEGet UserAttributes: gesplitste tunneling = gesplitste tunneling
	24 aug. 24:11:31:09 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, IKEGet UserAttributes: standaarddomein = jyoungta-labdomain.cisco.com
	24 aug. 24:11:31:09 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, IKEGet UserAttributes: IP-compressie = uitgeschakeld
	24 aug. 24:11:31:09 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam =

	gebruiker1, IP = 64.102.156.87, IKEGet UserAttributes: Split-tunneling-beleid uitgeschakeld 24 aug. 24:11:31:09 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, IKEGet UserAttributes: browser Proxy instellir = niet gewijzigd 24 aug. 24:11:31:09 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, IKEGet UserAttributes: Lokale proxy-passerin = uitschakelen 24 aug. 24:11:31:09 [IKEv1]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, gebruiker (gebruiker1) geauthentiseerd.
Verzend het resultaat.	24 aug. 24:11:31:09 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, voor het construeren van de lading met blanco hash 24 aug. 24:11:31:09 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, construerend qm hash payload-lading 24 aug. 24:11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE VERZENDingsbericht (msgid=5b6910ff) met payload: HDR + HASH (8) + ATT (14) + NONE (0) totale lengte: 64
	========== XAuth - Resultaat van autorisatie ==========">="="">
	5451:28:36.41608/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEven EV_XAUTHREQ_DONE 5461:28:36.41608/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEven EV_NO_EVENT 5471:28:36.42408/24/12002SV=Info/5IKE/0x630002F Ontvangen ISAKMP-pakket: peer = 64.102.156.88 5481:28:36.42408/24/12008=Info/4IKE/0x6300014 ONTVANGEN << ISAKMP OAK TRANS *(HASH, ATTR) vanaf 64.102.156.88 5491:28:36.42508/24/12-Sev=Decode/11IKE/0x6300001 ISAKMP-header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Volgende payload:slaan Ver (Hex):10 Exchange type:transactie Vlaggen:(Encryptie) MessageID(Hex):5B6910FF Lengte:76 payload-hash Volgende payload: Kenmerken Voorbehouden: 00 Lengte payload: 24 Gegevens (in hex): 7DCF47827164198731639BFB7595F694C9DDFE85 payload-kenmerken Volgende payload: None Voorbehouden: 00 Lengte payload: 12 Type: ISAKMP_CFG_SET Voorbehouden: 00 Identificatiecode: 0000 XAUTH-status: passeren 5501:28:36.42508/24/12 Sev=Debug/7IKE/0x6300076

	NAV-sporen ->TM:MsgID=5B6910FFCurState: TM_INITIALEvent: EV_RCVD_MSG 5511:28:36.42508/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_INIT_XAUTH 5211:28:36.42508/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_CHK_AUTH_RESULT
	5531:28:36.42508/24/12008=Info/4IKE/0x6300013 VERZENDING >> ISAKMP OAK TRANS *(HASH, ATTR) NAAR 64.102.156.8
	<==========" Xauth - Erkenning ==========">Erkenning
ACK ontvangen en verwerken; geen reactie van de server .	24 aug. 24:31:09 [IKEv1]IP = 64.102.156.87, ONTVANGEN IKE_DECODE Bericht (msgid=5b6910ff) met payload: HDR + HASH (8) + ATTR (14) + NONI (0) totale lengte: 60 24 aug. 24:11:31:09 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, process_attr(): Kom binnen! 24 aug. 24:11:31:09 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, Processing Cfg ACK-eigenschappen
	5511:28:36.42608/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_XAUTH_DONE_SUC 5611:28:36.42608/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_NO_EVENT 5711:28:36.42608/24/12008:2001:200000000000000000000 NAV-sporen ->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEven EV_TERM_REQUEST 5581:28:36.42608/24/12008:2001:2001:28:28:36:42608/24/12006 NAV-sporen ->TM:MsgID=FB709D4DCurState: TM_FREEvent: EV_REMOVE 5911:28:36.42608/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=FB709D4DCurState: TM_FREEvent: EV_NO_EVENT 5601:28:36.42608/24/12 Sev=Debug/7IKE/0x6300076 NAV Trace-9>SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_XAUTH_PROGEvent: EV_XAUTH_DONE_SUC 5611:28:38.4060/24/1208/12008=Debug/8IKE/0x630004C Start DPD-timer voor IKE SA (I_Cookie=D5619780D7BE3E5 R_Cookie=1B301D2DE710EDA0) sa->staat = 1, sa->dpd.bezorgd_freq(mSec = 5000 5621:28:38.40608/24/12008:2012 Sev=Debug/7IKE/0x6300076 NAV Trace-9>SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_MODECFG 5631:28:38.40608/24/12008:12-Sev=Debug/7IKE/0x6300076 NAV Trace-9>SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_NO_EVENT 5641:28:38.40608/24/12008:12-Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=84B4B653CurState: TM_INITIALEvent: EV_INIT_MODECFG 5651:28:38.408/24/1208:24/12:005E=Info/5IKE/0x630005E

	Cliënt die een firewallverzoek naar een concentrator stuurt 5611:28:38.40908/24/12008:24:12SEV=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_START_RETRY_TMR
	5671:28:38.40908/24/12008:24:12-Sev=Debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_SND_MSG 5681:28:38.40908/24/12008=Info/4IKE/0x6300013 VERZENDING >> ISAKMP OAK TRANS *(HASH, ATTR) NAAR 64.102.156.8 5691:28:38.62708/24/12 Sev=Decode/11IKE/0x6300001 ISAKMP-header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Volgende payload:slaan Ver (Hex):10 Exchange type:transactie Vlaggen:(Encryptie) MessageID (Hex):84B4B653 Lengte:183 payload-hash Volgende payload: Kenmerken Voorbehouden: 00 Lengte payload: 24 Gegevens (in hex): 81BF6721A744A815D69A315EF4AAA571D6B687 payload-kenmerken Volgende payload: None Voorbehouden: 00 Lengte payload: 131 Type: ISAKMP_CFG_REQUEST Voorbehouden: 00 Identificatiecode: 0000 IPv4-adres: (leeg) IPv4-netwerkmasker: (leeg) IPv4 DNS: (leeg) IPv4 NBS (WINS): (leeg) Adres: (leeg) Cisco-extensie: Banner: (leeg) Cisco-extensie: PWD opslaan: (leeg) Cisco-extensie: Standaard domeinnaam: (leeg) Cisco-extensie: Splitsen omvatten: (leeg) Cisco-extensie: DNS-naam splitsen: (leeg) Cisco-extensie: Voer PFS in: (leeg) Onbekend: (leeg) Cisco-extensie: Reserve-servers: (leeg) Cisco-extensie: Smart Card Verwijdering-verbinding: (leeg) Toepassingsversie: Cisco Systems VPN-client 5.0.07.290:WinNT Cisco-extensie: Firewalltype: (leeg) Cisco-extensie: Dynamische DNS-hostnaam: ATBASU-LABBOX
	<==========="Modus-configuratie"-aanvraag ==========="==="="Modus-configuratie")

Ontvang mode-enig verzoek.	24 aug. 24:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE ONTVANGEN Bericht (msgid=84b4b653) met payload: HDR + HASH (8) + ATTR (14) + NONE (0) totale lengte: 183 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, process_attr(): Kom binnen!	5701:28:38.6280/24/1200/12008/120011:28:38.6280/24/1200 NAV-sporen ->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_NO_EVENT
Procesmodus-configuratie verzoek. Veel van deze waarden worden gewoonlijk in het groepsbeleid geconfigureerd. Aangezien de server in dit voorbeeld echter een zeer basisconfiguratie heeft, zie je ze hier niet.	24 aug. 24:11:31:11 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, Eigenschappen voor verwerkingsaanvraag 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen verzoek om IPV4-adres! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvang het verzoek om IPV4 netmasker! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen aanvraag voor DNS-serveradres! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen aanvraag voor WINS server-adres 24 aug. 24:11:31:11 [IKEv1]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, ontvanger, niet-ondersteunde eigenschap transactiemodus: 5 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvang het verzoek om Banner! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen verzoek om instelling PW opslaan! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen aanvraag voor Default Domain Name! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen aanvraag voor splitter-tunnellijst! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen verzoek om DNS-splitter! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen aanvraag voor PFS-instelling! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP	

	= 64.102.156.87, MODE_CFG: Ontvangen aanvraag voor client-browser Prox instelling! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen aanvraag voor een reservekopie va ip-sec peer list! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen aanvraag voor client-Smartcard- verwijderingsinstelling voor verbroken verbinding! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen aanvraag voor toepassingsversie! 24 aug. 24:11:31:11 [IKEv1]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, clienttype: WinNTClient-toepassing versie: 5.0.07.0290 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen aanvraag voor FWTYPE! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, MODE_CFG: Ontvangen aanvraag voor DHCP-hostname voor DDNS is: ATBASU-LABBOX!
Construct mode-configuratie antwoord met alle waarden die worden gevormd. Relevante configuratie: In dit geval wordt de gebruiker altijd dezelfde IP toegewezen. 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 aug. 24:11:31:11 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, verkregen IP-adres (192.168.1.100) voorafgaand aan het openen van mode Cfg (XAth) 24 aug. 24:1:31:11 [IKEv1 DEBUG]Group = ipsec, Username = gebruiker1, IP 64.102.156.87, Sending SUBNET-masker (255.255.255.0) naar externe client 24 aug. 24:11:31:11 [IKEv1]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, toegewezen privé IP-adres 192.168.1.100 aan externe gebruiker 24 aug. 24:11:31:11 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, voor het construeren van de lading met blanco hash 24 aug. 24 11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, construct_cfg_set: standaarddomein = jyoungta- labdomain.cisco.com 24 aug. 24:11:31:11 [IKEv1 DEBUG]Group = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, client-browser proxy kenmerken! 24 aug. 24:11:31:11 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, browser proxy ingesteld op No-Wijzigen. De gegevens van c browser worden NIET in het mode-cfg antwoord opgenomen 24 aug. 24:11:31:11 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, Verzend Cisco SmartCard-verwijderingsvenster voor!! 24 aug. 24:11:31:11 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, construerend qm hash payload-lading
Verzend de wijze-configuratie respons.	24 aug. 24:11:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE VERZENDingsbericht (msgid=84b4b653) met payload: HDR + HASH (8) + ATTR (14) + NONE (0) totale lengte: 215
	==========="Modus-configuratie-respons ==========="====>
	5711:28:38.6380/24/12008=Info/5IKE/0x630002F Ontvangen ISAKMP-pakket: peer = 64.102.156.88 5721:28:38.6380/24/12008=Info/4IKE/0x6300014 ONTVANGEN << ISAKMP OAK TRANS *(HASH, ATTR) vanaf 64.102.156.88

		5731:28:38.63908/24/12 Sev=Decode/11IKE/0x6300001 ISAKMP-header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Volgende payload:slaan Ver (Hex):10 Exchange type:transactie Vlaggen:(Encryptie) MessageID (Hex):84B4B653 Lengte:220 payload-hash Volgende payload: Kenmerken Voorbehouden: 00 Lengte payload: 24 Gegevens (in hex): 6DE2E70ACF6B185846BC62E590C00A6745D14D payload-kenmerken Volgende payload: None Voorbehouden: 00 Lengte payload: 163 Type: ISAKMP_CFG_REPLY Voorbehouden: 00 Identificatiecode: 0000 IPv4-adres: 192.168.1.100 IPv4-netwerkmasker: 255.255.255.0 IPv4 DNS: 192.168.1.99 Cisco-extensie: PWD opslaan: Nee Cisco-extensie: Standaard domeinnaam: jyoungta-labdomain.cisco.com Cisco-extensie: Voer PFS in: Nee Toepassingsversie: Cisco Systems, Inc. ASA 5505 versie 8.4(4)1 gebouwd door bouders op Thu 14-Jun-12 11:20 Cisco-extensie: Smart Card Verwijdering-verbinding: Ja
Fase 1 wordt op server voltooid. Start Quick Mode (QM)-proces.	24 aug. 24:11:31:13 [IKEv1 DECODE]IP = 64.102.156.87, IKE-responder met QM: msg-id = 0e83792e 24 aug. 24:11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = gebruiker1, IP = 64.102.156.87, Delay Quick Mode bewerking, Cert/Trans	5741:28:38.63908/24/12008/120000076 NAV-sporen ->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_RCVD_MSG 5751:28:38.63908/24/12008/1200010 Info/5IKE/0x6300010 MODE_CFG_REPLY: Kenmerk = INTERNAL_IPV4_ADRES:, waarde = 192.168.1.100 5761:28:38.63908/24/12 Sev=Info/5IKE/0x6300010 MODE_CFG_REPLY: Kenmerk = INTERNAL_IPV4_NETMASK:, waarde = 255,255,255,0 5771:28:38.63908/24/12008/1200010 Info/5IKE/0x6300010 MODE_CFG_REPLY: Kenmerk = INTERNAL_IPV4_DNS(1): , waarde = 192.168.1.99 5781:28:38.63908/24/12000SV=Info/5IKE/0x630000D MODE_CFG_REPLY: Kenmerken = MODECFG_UNITY_SAVEPWD: , waarde = 0x00000000 5791:28:38.63908/24/12000E=Info/5IKE/0x630000E MODE_CFG_REPLY: Kenmerken = MODECFG_UNITY_DEFDOMAIN: , waarde = jyoungta-labdomain.cisco.com 5801:28:38.63908/24/12000S-L= Info/5IKE/0x630000D

	Exch/RM DSID in uitvoering 24 aug. 24:11:31:13 [IKEv1]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, Gratuitachtige ARP verstuurd voor 192.168.1.100 24 aug. 24:11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = gebruiker1, IP = 64.102.156.87, Resume Quick Mode bewerking, Cert/Trans Exch/RM DSID voltooid 24 aug. 24:11:31:13 [IKEv1]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, FASE 1 VOLTOOID	MODE_CFG_REPLY: Attribuut = MODECFG_UNITY_PFS: , waarde = 0x00000000 5811:28:38.63908/24/12000E=Info/5IKE/0x630000E MODE_CFG_REPLY: Kenmerk = APPLICATION_VERSIE waarde = Cisco Systems, Inc ASA 5505 versie 8.4(4)1 gebouwd door bouwers op Thu 14-Jun-12 11:20 5821:28:38.63908/24/12000SV= Info/5IKE/0x630000D MODE_CFG_REPLY: Kenmerken = MODECFG_UNITY_SMARTCARD_REMOVAL_DISCONNEC , waarde = 0x00000001 5831:28:38.63908/24/12000S-L= Info/5IKE/0x630000D MODE_CFG_REPLY: Kenmerk = ontvangen en gebruikt NAT-havennummer, waarde = 0x0001194 5841:28:39.36708/24/12 Sev= Debug/9IKE/0x6300093 Waarde voor ini-parameter EnableDNSRedirectie is 1 5851:28:39.36708/24/12008/1200076 debug/7IKE/0x6300076 NAV-sporen ->TM:MsgID=84B4B653CurState: TM_MODECFG_DONEEvent: EV_MODECFG_DONE_SUC
Constructeren en sturen DPD voor client.	24 aug. 24:11:31:13 [IKEv1]IP = 64.102.156.87, type bewaar voor deze verbinding: DPD 24 aug. 24:11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = gebruiker1, I = 64.102.156.87, Starttimer P1 rekey: 82080 seconden. 24 aug. 24:11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = gebruiker1, I = 64.102.156.87, bericht van kennisgeving verzenden 24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, voor het construeren van de lege hashlading 24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, construerend qm hash payload-lading 24 aug. 24:11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Message (msgid=be8f7821) met payload: HDR + HASH (8) + MEDEDELING	

	(11) + NIET (0) totale lengte: 92
	========== detectie van dial-peers (DPD) ==========>=====">)
	5811:28:39.79508/24/12 Sev=Debug/7IKE/0x6300015 intf_data: lcl=0x0501A8C0, masker=0x00FFFF, bcast=0xFF01A8C0, bcast_vra=0xFF070A 5891:28:39.79508/24/12 Sev=Debug/7IKE/0x6300076 NAV Trace-9>SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_P2 5901:28:39.79508/24/12008=Info/4IKE/0x6300056 Ontvang een sleutelverzoek van Stuurprogramma: Lokale IP = 192.168.1.100 GW IP = 64.102.156.88, externe IP = 0.0.0 5911:28:39.79508/24/12008:12-Sev=Debug/7IKE/0x6300076 NAV Trace-9>SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_ACTIVEEvent: EV_NO_EVENT 5921:28:39.79508/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->QM:MsgID=0E83792ECurState: QM_INITIALEvent: EV_INITIATOR 5931:28:39.79508/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->QM:MsgID=0E83792ECurState: Event van QM_BLD_MSG: EV_CHK_PFS 5941:28:39.79608/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->QM:MsgID=0E83792ECurState: Event van QM_BLD_MSG: EV_BLD_MSG 595 11:28:39.79608/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->QM:MsgID=0E83792ECurState: Event van QM_SND_MSG1Event: EV_START_RETRY_TMR
	5961:28:39.79608/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->QM:MsgID=0E83792ECurState: Event van QM_SND_MSG1Event: EV_SND_MSG 5971:28:39.79608/24/12 Sev=Info/4IKE/0x6300013 VERZENDING >> ISAKMP OAK QM *(HASH, SA, NON, ID) TOT 64.102.156.88
	<==========="#Snel mode Berichtje 1 (QM1) ==========="="="="="="="="="="="="="=")
Ontvang QM1.	24 aug. 24:31:13 [IKEv1]IP = 64.102.156.87, ONTVANGEN IKE_DECODE Bericht (msgid=e83792e) met payload: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) totale lengte: 1026
Verwerking van QM1. Relevante configuratie: `crypto dynamic-map DYN 10 set transform-set TRA`	24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, verwerkingspremie lading 24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, verwerking van SA-lading 24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, verwerking eenmaal payload 24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, verwerkings-ID-lading 24 aug. 24:11:31:13 [IKEv1 DECODE]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, ID_IPV4_ADDR ontvangen ID 192.168.1.100 24 aug. 24:11:31:13 [IKEv1]groep = ipsec, gebruikersnaam = gebruiker1, IP =

	64.102.156.87, ontvangen externe proxy-hostgegevens in ID-payload:Adres 192.168.1.100, Protocol 0, poort 0 24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, verwerkings-ID-lading 24 aug. 24:11:31:13 [IKEv1 DECODE]Group = ipsec, Username = gebruiker1, IP = 64.102.156.87, ID_IPV4_ADDR_SUBNET ID ontvangen—0.0.0—0.0.0.0 24 aug. 24:11:31:13 [IKEv1]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, ontvangen lokale IP-proxysubnetgegevens in ID payload:adres 0.0.0, masker 0.0.0.0, protocol 0, poort 0 24 aug. 24:11:31:13 [IKEv1]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, QM isRekeyed old zoals niet door addr gevonden 24 aug. 24:11:31:13 [IKEv1]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, Static Crypto Map check, check map = out-map, seq = 10.... 24 aug. 24:11:31:13 [IKEv1]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, Static Crypto Map Check by-pass: Crypto map entry incomplet 24 aug. 24:11:31:13 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, uitsluitend UDP-ingekapselde tunnelen en UDP-ingekapseld transportmodi geselecteerd door NAT-verkeer 24 aug. 24:11:31:13 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, uitsluitend UDP-ingekapselde tunnelen en UDP-ingekapseld transportmodi geselecteerd door NAT-verkeer 24 aug. 24:11:31:13 [IKEv1]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, IKE Remote Peer ingesteld voor crypto-kaart: in kaart brenger 24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, verwerking van IPSec SA-lading

Bevestig QM2.
Relevante configuratie:
 	
`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 aug. 24:11:31:13 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, IPSec SA Voorstel # 12, Transformeer # 1 acceptabeleMatches wereldwijde IPSec SA-ingang # 10
	24 aug. 24:11:31:13 [IKEv1]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, IKE: SPI eisen!
	IPSEC: Nieuwe embryonaal SA, gecreëerd bij 0xcfdffc90,
	SCB: 0xCFDFFB58, Richting: binnenkomend
	SPI: 0x9E18ACB2
	Session-id: 0x00138000
	VPIF num: 0x0000004
	Tunneltype: ra
	Protocol: esp
	Levensduur: 240 seconden
	24 aug. 24:11:31:13 [IKEv1 DEBUG]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, IKE kreeg SPI van de sleutelmotor: SPI = 0x9e18acb2
	24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, oakley die de snelle modus bouwt
	24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, voor het construeren van de lege hashlading
	24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, waarbij IPSec SA-lading wordt geconstrueerd
	24 aug. 24:11:31:13 [IKEv1]Groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, herroepingsduur IPSec Initiator van 2147483 tot 86400 seconden
	24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, waarbij IPSec nonce werd geconstrueerd
	24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, waarbij proxy-ID wordt geconstrueerd

	24 aug. 24:11:31:13 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, proxy-id voor verzending: Remote-host: 192.168.1.100 Protocol 30-poorts 10 Plaatselijke subnetwerken:0.0.0.0masker 0.0.0.0 Protocol 0-poorts 0.0 24 aug. 24:11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = gebruiker1, I = 64.102.156.87, verzend RESPONDER LIFETIME kennisgeving aan Initiator 24 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I = 64.102.156.87, construerend qm hash payload-lading
Verzend QM2.	24 aug. 24:11:31:13 [IKEv1 DECODE]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, IKE-responder verzenden tweede QM-pakket: msg-id = 0e83792e 24 aug. 24:11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE VERZENDingsbericht (msgid=e83792e) met payload: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + MEDEDELING (11) + GEEN (0) totale lengte : 184
	==========**"#Snel mode-bericht 2 (QM2)** ==========**">=">)**
	6081:28:39.96208/24/12008=Info/4IKE/0x6300014 ONTVANGEN << ISAKMP OAK QM *(HASH, SA, NON, ID, ID, MELDING: STATUS_RESP_LIFETIME) VAN 64.102.156.88
	6091:28:39.96408/24/12001 Sev=Decode/11IKE/0x6300001 ISAKMP-header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Volgende payload:slaan Ver (Hex):10 Exchange type:Quick Mode Vlaggen:(Encryptie) MessageID(Hex):E83792E Lengte:188 payload-hash Volgende payload: Security Association Voorbehouden: 00 Lengte payload: 24 Gegevens (in hex): CABF38A62C9B88D1691E81F3857D6189534B2EC0 payload-beveiligingsassociatie Volgende payload: Nonce Voorbehouden: 00 Lengte payload: 52 DOI: IPsec Situatie: (SIT_IDENTITY_ONLY) payloadvoorstel Volgende payload: None Voorbehouden: 00 Lengte payload: 40 Voorstel nr.: 1 Protocol-ID: PROTEST_IPSEC_ESP SPI-grootte: 4 # transformatie: 1 SPI: 9E18ACB2 payloadtransformatie

	Volgende payload: None Voorbehouden: 00 Lengte payload: 28 Omzetten #: 1 ID omzetten: ESP_3DES Voorbehouden2: 0000 Levenstype: seconden Levensduur (hex): 0020C49B Insluitingsmodus: UDP-tunnels Verificatiealgoritme: SHA1 Payload Nonce Volgende payload: Identificatie Voorbehouden: 00 Lengte payload: 24 Gegevens (in hex): 3A079B75DA512473706F235EA3FCA61F1D15D4CD Identificatie van payload Volgende payload: Identificatie Voorbehouden: 00 Lengte payload: 12 ID type: IPv4-adres Protocol-ID (UDP/TCP, enzovoort): 0 Port: 0 ID-gegevens en -kolommen; 192.168.1.100 Identificatie van payload Volgende payload: Kennisgeving Voorbehouden: 00 Lengte payload: 16 ID type: IPv4-subnet Protocol-ID (UDP/TCP, enzovoort): 0 Port: 0 ID-gegevens en -kolommen; 0.0.0.0/0.0.0.0 payloadmelding Volgende payload: None Voorbehouden: 00 Lengte payload: 28 DOI: IPsec Protocol-ID: PROTEST_IPSEC_ESP Centrifugegrootte: 4 Type melding: STATUS_RESP_LIFETIME SPI: 9E18ACB2 Gegevens en analyse; Levenstype: seconden Levensduur (hex): 00015180
	6101:28:39.96508/24/12008:240000000000000000000000000 NAV-sporen ->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Event: EV_RCVD_MSG 6111:28:39.96508/24/12008=Info/5IKE/0x6300045 RESPONDER-LIFETIME notification heeft een waarde van 86400 seconden 612:11:28:39.96508/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Event: EV_CHK_PFS 613:11:28:39.96508/24/12008:2012 Sev=Debug/7IKE/0x6300076
	NAV-sporen ->QM:MsgID=0E83792ECurState: QM_BLD_MSG3Event:

	EV_BLD_MSG 614:11:28:39.96508/24/12 Sev=Debug/7IKE/0x6300076 ISAKMP-header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Volgende payload:slaan Ver (Hex):10 Exchange type:Quick Mode Vlaggen:(Encryptie) MessageID(Hex):E83792E Lengte:52 payload-hash Volgende payload: None Voorbehouden: 00 Lengte payload: 24 Gegevens (in hex): CDDC20D91EB4B568C826D6A5770A5CF020141236
	615:11:28:39.96508/24/12 Sev=Debug/7IKE/0x6300076 NAV-sporen ->QM:MsgID=0E83792ECurState: QM_SND_MSG3Event: EV_SND_MSG 616:11:28:39.96508/24/12008=Info/4IKE/0x6300013 VERZENDING >> ISAKMP OAK QM *(HASH) NAAR 64.102.156.88
	<==========="#Snel mode-bericht 3 (QM3) ==========="=")
Ontvang QM3.	24 aug. 24:31:13 [IKEv1]IP = 64.102.156.87, ONTVANGEN IKE_DECODE Bericht (msgid=e83792e) met payload: HDR + HASH (8) + NONE (0) totale lengte: 52

ProcesQM3. Maak de inkomende en uitgaande security parameter-indexen (SPI's). Voeg statische route voor de gastheer toe.
Relevante configuratie:
 	
`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 aug. 24:11:31:13 [IKEv1 DEBUG]Groep = ipsec, Username = gebruiker1, I
	= 64.102.156.87, verwerkingspremie lading
	24 aug. 24:11:31:13 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, alle IPSEC SA's laden
	24 aug. 24:11:31:13 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, genererende sneltoets!
	24 aug. 24:11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = gebruiker1, I
	= 64.102.156.87, NP-encryptie regelt het zoeken naar crypto-kaart out-dyn-ma
	10 matching ACL onbekend: teruggestuurd
	cs_id=cc107410; regel=000000000
	24 aug. 24:11:31:13 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, genererende sneltoets!
	IPSEC: Nieuwe embryonaal-SA gemaakt bij 0xcc9ed60,
	SCB: 0xCF7F59E0,
	Richting: uitgaand
	SPI: 0xC052-90A
	Session-id: 0x00138000
	VPIF num: 0x0000004
	Tunneltype: ra
	Protocol: esp
	Levensduur: 240 seconden
	IPSEC: Voltooide host OBSA-update, SPI 0xC055290A
	IPSEC: Een uitgaande VPN-context maken, SPI 0xC05290A
	Vlaggen: 0x0000025
	SA: 0xcc9ed60
	SPI: 0xC052-90A

	MTU: 1500 bytes VCID : 0x0000000 Peer : 0x0000000 SCB: 0xA5922B6B Kanaal: 0xc82afb60 IPSEC: Volledig uitgaande VPN-context, SPI 0xC05290A VPN-handle: 0x0015909c IPSEC: Nieuwe uitgaande versleutelde regel, SPI 0xC05290A src-adres: 0.0.0.0 Src-masker: 0.0.0.0 addr.: 192.168.1.100 Tekstmasker: 255.255.255.255 Src-poorten Bovenkant: 0 Lager: 0 Op: negeren Startpoorten Bovenkant: 0 Lager: 0 Op: negeren Protocol: 0 Protocol gebruiken: onjuist SPI: 0x0000000 SPI gebruiken: onjuist IPSEC: Volledig uitgaande versleuteling, SPI 0xC05290A Regel ID: 0xcb47a710 IPSEC: Nieuwe regel voor uitgaande vergunningen, SPI 0xC05290A src-adres: 64.102.156.88 Src-masker: 255.255.255.255 addr.: 64.102.156.87 Tekstmasker: 255.255.255.255 Src-poorten Bovenkant: 4500 Lager: 4500 Op: gelijk Startpoorten Bovenkant: 58506 Lager: 58506 Op: gelijk Protocol: 17 Protocol gebruiken: reëel SPI: 0x0000000 SPI gebruiken: onjuist IPSEC: Ingevulde uitgaande vergunningsregel, SPI 0xC05290A Regel ID: 0xcdf3cfa0 24 aug. 24:11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = gebruiker1, I = 64.102.156.87, NP-encryptie regelt het zoeken naar crypto-kaart out-dyn-ma 10 matching ACL onbekend: teruggestuurd cs_id=cc107410; regel=000000000 24 aug. 24:11:31:13 [IKEv1]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, Security onderhandeling voltooid voor gebruiker (gebruiker1)Responder, Inbound SPI = 0x9e18acb2, Uitgaande SPI = 0xc055290a

	24 aug. 24:11:31:13 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, IKE kreeg een KEY_ADD msg voor SA: SPI = 0xc055290a IPSEC: Voltooide host IBSA-update, SPI 0x9E18ACB2 IPSEC: Een inkomende VPN-context maken, SPI 0x9E18ACB2 Vlaggen: 0x0000026 SA: 0xcfdffc90 SPI: 0x9E18ACB2 MTU: 0 bytes VCID : 0x0000000 Peer : 0x0015909c SCB: 0xA5672481 Kanaal: 0xc82afb60 IPSEC: Voltooide inkomende VPN-context, SPI 0x9E18ACB2 VPN-handle: 0x0016219c IPSEC: Bijwerken van uitgaande VPN-context 0x0015909C, SPI 0xC05290A Vlaggen: 0x0000025 SA: 0xcc9ed60 SPI: 0xC052-90A MTU: 1500 bytes VCID : 0x0000000 Peer : 0x0016219c SCB: 0xA5922B6B Kanaal: 0xc82afb60 IPSEC: Volledig uitgaande VPN-context, SPI 0xC05290A VPN-handle: 0x0015909c IPSEC: Volledig uitgaande binnenregel, SPI 0xC05290A Regel ID: 0xcb47a710 IPSEC: Voltooide buitenste SPD-regel, SPI 0xC05290A Regel ID: 0xcdf3cfa0 IPSEC: Nieuwe regels voor inkomende tunnelstromen, SPI 0x9E18ACB2 src-adres: 192.168.1.100 Src-masker: 255.255.255.255 addr.: 0.0.0.0 Tekstmasker: 0.0.0.0 Src-poorten Bovenkant: 0 Lager: 0 Op: negeren Startpoorten Bovenkant: 0 Lager: 0 Op: negeren Protocol: 0 Protocol gebruiken: onjuist SPI: 0x0000000 SPI gebruiken: onjuist IPSEC: Voltooide inkomende tunnelstroomregel, SPI 0x9E18ACB2 Regel ID: 0xDF15270 IPSEC: Nieuwe regel voor inkomende decryptie, SPI 0x9E18ACB2 src-adres: 64.102.156.87 Src-masker: 255.255.255.255 addr.: 64.102.156.88

	Tekstmasker: 255.255.255.255 Src-poorten Bovenkant: 58506 Lager: 58506 Op: gelijk Startpoorten Bovenkant: 4500 Lager: 4500 Op: gelijk Protocol: 17 Protocol gebruiken: reëel SPI: 0x0000000 SPI gebruiken: onjuist IPSEC: Voltooide decryptie regel, SPI 0x9E18ACB2 Regel ID: 0xce30c2f8 IPSEC: Nieuwe regel voor inkomende vergunningen, SPI 0x9E18ACB2 src-adres: 64.102.156.87 Src-masker: 255.255.255.255 addr.: 64.102.156.88 Tekstmasker: 255.255.255.255 Src-poorten Bovenkant: 58506 Lager: 58506 Op: gelijk Startpoorten Bovenkant: 4500 Lager: 4500 Op: gelijk Protocol: 17 Protocol gebruiken: reëel SPI: 0x0000000 SPI gebruiken: onjuist IPSEC: Ingevulde vergunningsregel, SPI 0x9E18ACB2 Regel ID: 0xcf6f58c0 24 aug. 24:11:31:13 [IKEv1 DEBUG]groep = ipsec, gebruikersnaam = gebruiker1, IP = 64.102.156.87, Pitcher: ontvangen KEY_UPDATE, spi 0x9e18acb2 24 aug. 24:11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = gebruiker1, I = 64.102.156.87, Starttimer P2 rekey: 82080 seconden. 24 aug. 24:11:31:13 [IKEv1]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, statische route toevoegen voor clientadres: 192.168.1.100
Fase 2 voltooid. Beide partijen versleutelen en decrypteren nu.	24 aug. 24:11:31:13 [IKEv1]groep = ipsec, Username = gebruiker1, IP = 64.102.156.87, FASE 2 COMPLETED (msgid=0e83792e)
Voor hardwareklanten wordt nog één bericht ontvangen waar de klant informatie over zichzelf versturen. Als u zorgvuldig kijkt, zou u de hostname van de EzVPN client, software moeten vinden die op de client	24 aug. 24:31:13 [IKEv1]: IP = 10.48.66.23, IKE_DECODE ONTVANGEN Bericht (msgid=91facca9) met lading: HDR + HASH (8) + MEDEDELING (11) NIET (0) totale lengte: 184 24 aug. 24:31:13 [IKEv1 DEBUG]: Groep = EZ, Gebruikersnaam = cisco, IP = 10.48.66.23, verwerkingspremie 24 aug. 24:31:13 [IKEv1 DEBUG]: Groep = EZ, Gebruikersnaam = cisco, IP = 10.48.66.23, verwerkingskennisgeving voor lading 24 aug. 24:31:13 [IKEv1 DECODE]: VEROUDERDE BESCHRIJVING - INDEX 1

wordt uitgevoerd en de locatie en naam van de software	24 aug. 24:31:13 [IKEv1 DECODE]: 0000: 00000000 7534000B 62736E73 2D383731 ...,u4.**bng-871** 0010: 2D332E75 32000943 6973636F 20383731 **-3**.u2..**Cisco 871** 0020: 7535000B 46484B30 393431 32513675 u5.FHK094412Q6u 0030: 36000932 32383538 39353638 75390009 6..228589568u 9... 0040: 31343532 3136331 32753300 2B666C61 145216312u3.+**fla** 0050: 73683A63 3837302D 6164769 70736572 **sh:c870-adviseur** 0060: 7696365 736B392D 6A2E31 32342D32 **vicesk9-mz.124-2** 0070: 302E5435 2E62696E **0.T5.2000** 24 aug. 24:31:13 [IKEv1 DEBUG]: Groep = EZ, Gebruikersnaam = cisco, IP = 10.48.66.23, PSK-hash verwerken 24 aug. 24:31:13 [IKEv1]: Groep = EZ, Gebruikersnaam = cisco, IP = 192.168.1.100, Onconsistente PSK-hasgrootte 24 aug. 24:31:13 [IKEv1 DEBUG]: Group = EZ, Username = cisco, IP = 10.48.66.23, PSK Hash Verification mislukt!

Tunnelverificatie

ISAKMP

Uitvoer van de **sh wenen is sa det** commando:

```
 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

Aangezien het Internet Control Message Protocol (ICMP) wordt gebruikt om de tunnel te activeren, is slechts één IPsec SA geactiveerd. Protocol 1 is ICMP. Merk op dat de SPI-waarden verschillen van die welke in de debugs zijn onderhandeld. Dit is in feite dezelfde tunnel na de tweede fase.

Uitvoer van de **sh crypto ipsec** opdracht is:

```
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
```

Gerelateerde informatie

- Wikipedia-artikel over IPsec
- IPsec-probleemoplossing: Opdrachten begrijpen en gebruiken
- Technische ondersteuning en documentatie – Cisco Systems