Note technique de dépannage des débogages ASA IPsec et IKE (IKEv1 Aggressive Mode)

Contenu

Introduction

Ce document décrit les débogages sur l'appareil de sécurité adaptatif Cisco (ASA) lorsque le mode agressif et la clé prépartagée (PSK) sont utilisés. La traduction de certaines lignes de débogage dans la configuration est également abordée. Cisco vous recommande d'avoir une connaissance de base d'IPsec et d'Internet Key Exchange (IKE).

Ce document ne traite pas du trafic de passage après l'établissement du tunnel.

Problème principal

Les débogages IKE et IPsec sont parfois cryptiques, mais vous pouvez les utiliser afin de comprendre les problèmes avec l'établissement du tunnel VPN IPsec.

Scénario

Le mode agressif est généralement utilisé dans le cas d'Easy VPN (EzVPN) avec le logiciel (client VPN Cisco) et les clients matériels (dispositif de sécurité adaptatif Cisco ASA 5505 ou Cisco IOS ? Les routeurs logiciels), mais uniquement lorsqu'une clé pré-partagée est utilisée. Contrairement au mode principal, le mode agressif consiste en trois messages.

Les débogages proviennent d'un ASA qui exécute le logiciel version 8.3.2 et agit en tant que serveur EzVPN. Le client EzVPN est un client logiciel.

Commandes debug utilisées

Voici les commandes debug utilisées dans ce document :

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

Configuration ASA

La configuration ASA dans cet exemple est conçue comme étant strictement de base ; aucun serveur externe n'est utilisé.

```
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
```

Débogage

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Description du message du serveur	Déboguages		Description du message client
	49711:28:30.28908/24/12Sev=Info/6IKE/0x6300003B Tentative d'établissement d'une connexion avec 64.102.156.88. 49811:28:30.29708/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState : AM_INITIALEvent : EV_INITIATEUR 49911:28:30.29708/24/12Sev=Info/4IKE/0x63000001 Démarrage de la négociation IKE de phase 1 50011:28:30.29708/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState : AM_SND_MSG1Événement : EV_GEN_DHKEY 50111:28:30.30408/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState : AM_SND_MSG1Événement : EV_BLD_MSG 50211:28:30.30408/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState : AM_SND_MSG1Événement : EV_START_RETRY_TMR 50311:28:30.30408/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState : AM_SND_MSG1Événement : EV_SND_MSG		Le mode agressif démarre. Construisez AM1. Ce processus comprend : - ISAKMP HDR - Dispositif de sécurité (SA) contenant toutes les charges utiles de transformation et les propositions prises en charge par le client - Charge utile Exchange de clé - ID initiateur de phase 1 - Nonce
	50411:28:30.30408/24/12Sev=Info/4IKE/0x63000013 ENVOI » ISAKMP OAK AG (SA, KE, NON, ID, VID(Xauth), VID(dpd), VID(Frag), VID(Nat-T), VID(Unity)) à 64.102.156.88		Envoyer AM1.
	<========== Message 1 agressif (AM1) ==========		
Recevez AM1 du client.	24 août 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=0) avec charges utiles : HDR + SA (1) +	50611:28:30.3308/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState : AM_WAIT_MSG2Event : EV_NO_EVENT	Attendez la réponse du serveur.

	KE (4) + NONCE (10) + ID (5) + FOURNISSEUR (13) + FOURNISSEUR (13) + FOURNISSEUR (13) + FOURNISSEUR (13) + FOURNISSEUR (13) + AUCUNE (0) longueur totale : 849		

Traiter AM1. Comparer les propositions reçues et les transformations avec celles déjà configurées pour les correspondances. Configuration appropriée : ISAKMP est activé sur l'interface, et au moins une stratégie est définie qui correspond à ce que le client a envoyé :
 	
`crypto isakmp enable outside`
`crypto isakmp policy 10`
`authentication pre-share`
`encryption aes`
`hash sha`
`group 2`
`lifetime 86400`
Groupe de tunnels correspondant au nom d'identité présent :
 	
`tunnel-group EZ type remote-access`
`tunnel-group EZ general-attributes`
`default-group-policy EZ`
`tunnel-group EZ ipsec-attributes`
	24 août 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, traitement de la charge utile SA
	24 août 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, traitement de la charge utile principale
	24 août 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, traitement de la charge utile ISA_KE
	24 août 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, traitement de la charge utile nonce
	24 août 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, charge utile d'ID de traitement
	24 août 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, traitement de la charge utile VID
	24 août 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, reçu VID xauth V6
	24 août 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, traitement de la charge utile VID
	24 août 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, VID DPD reçu
	24 août 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, traitement de la charge utile VID
	24 août 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, VID de fragmentation reçu
	24 août 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, IKE Peer inclut les indicateurs de capacité de fragmentation IKE : Mode principal:Mode TrueAggressive:False
	24 août 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, traitement de la charge utile VID
	24 août 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, VID NAT-Traversal ver 02 reçu
	24 août 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, traitement de la charge utile VID
	24 août 11:31:03 [DEBUG IKEv1]IP = 64.102.156.87, VID client Cisco Unity reçu
	24 août 11:31:03 [IKEv1]IP = 64.102.156.87, Connection a atterri sur tunnel_group ipsec
	24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, traitement de la charge utile IKE SA	

pre-shared-key cisco	24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1]Échec de la phase 1 : types d'attributs non concordants pour la classe Description du groupe : Rcv'd : Groupe 2Cfg : Groupe 5 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, proposition IKE SA n° 1, Transformation n° 5 acceptableCorrespondances entrée IKE n° 1 globale	
Construisez AM2. Ce	24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP =	

processus comprend : - les politiques choisies - Diffie-Hellman (DH) - ID du répondeur -authentification - Charge utile de détection NAT (Network Address Translation)	64.102.156.87, construction de la charge utile ISAKMP SA 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de la charge utile principale 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de la charge utile nonce 24 août 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Génération de clés pour Responder... 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de la charge utile ID 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de la charge utile de hachage 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, hachage de calcul pour ISAKMP 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de la charge utile Cisco Unity VID 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de la charge utile VID xauth V6 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de la charge utile dpd vid 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de la charge utile NAT-Traversal VID ver 02 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de la charge utile NAT-Discovery 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, calcul du hachage de découverte NAT 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de la charge utile NAT-Discovery 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, calcul du hachage de découverte NAT 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de Fragmentation VID + charge utile de fonctionnalités étendues 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de la charge utile VID 24 août 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Send Altiga/Cisco VPN3000/Cisco ASA GW VID	
Envoyer AM2.	24 août 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE ENVOI du message (msgid=0) avec les charges utiles : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDEUR (13) + VENDEUR (13) + VENDEUR (13) + VENDEUR (13) + NAT-D (130) + NAT-D (130) + VENDOR (1) 3) + FOURNISSEUR (13) + AUCUNE (0) longueur totale : 444	
	========== Message 2 agressif (AM2) ==========>	

	50711:28:30.40208/24/12Sev=Info/5IKE/0x6300002F Paquet ISAKMP reçu : homologue = 64.102.156.8 50811:28:30.40308/24/12Sev=Info/4IKE/0x63000014 REÇU «< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID(Unity), VID(Xauth), VID(dpd), VID(Nat-T), NAT-D, NAT-D, VID(Frag), VID(?)) à partir de 64.102.156.8 8 51011:28:30.41208/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_WAIT_MSG2Event : EV_RCVD_MSG	Recevez AM2.
	51111:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Peer est un homologue conforme à Cisco-Unity 51211:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Prise en charge XAUTH par les homologues 51311:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Prise en charge DPD par les homologues 51411:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Peer-support NAT-T 51511:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Les homologues prennent en charge les charges utiles de fragmentation IKE 51611:28:30.41208/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_WAIT_MSG2Event : EV_GEN_SKEYID 51711:28:30.42208/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_WAIT_MSG2Event : EV_AUTHENTICATE_PEER 51811:28:30.42208/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_WAIT_MSG2Event : EV_AJUSTER_PORT 51911:28:30.42208/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_WAIT_MSG2Event : EV_CRYPTO_ACTIVE	Processus AM 2.
	52011:28:30.42208/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_SND_MSG3Événement : EV_BLD_MSG] 52111:28:30.42208/24/12Sev=Débogage/8IKE/0x63000001 Démarrage de la construction de l'ID fournisseur IOS 52211:28:30.42208/24/12Sev=Info/6IKE/0x63000001 La construction de l'ID du fournisseur IOS a réussi	Construisez AM3. Ce processus inclut l'authentification du client. À ce stade, toutes les données pertinentes pour le chiffrement ont déjà été échangées.

	52311:28:30.42308/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_SND_MSG3Événement : EV_SND_MSG 52411:28:30.42308/24/12Sev=Info/4IKE/0x63000013 ENVOI » ISAKMP OAK AG *(HASH, NOTIFY : STATUS_INITIAL_CONTACT, NAT-D, NAT-D, VID(?), VID(Unity)) à 64.102.156.88	Envoyer AM3.
	<========== Message 3 agressif (AM3) ==========	
Recevez AM3 du client.	24 août 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=0) avec charges utiles : HDR + HASH (8) + NOTIFICATION (11) + NAT-D (130) + NAT-D (130) + FOURNISSEUR (13) + FOURNISSEUR (13) + AUCUNE (0) longueur totale : 168	
Processus AM 3. Confirmez l'utilisation de NAT traversal (NAT-T). Les deux parties sont maintenant prêtes à commencer le cryptage du trafic.	24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, traitement des données utiles de hachage 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, hachage de calcul pour ISAKMP 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, traitement de la charge utile de notification 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, traitement de la charge utile NAT-Discovery 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, calcul du hachage de découverte NAT 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, traitement de la charge utile NAT-Discovery 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, calcul du hachage de découverte NAT 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, traitement de la charge utile VID 24 août 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Traitement de la charge utile IOS/PIX ID fournisseur (version : 1.0.0, fonctionnalités : 00000408) 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, traitement de la charge utile VID 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, reçu VID du client Cisco Unity 24 août 11:31:03 [IKEv1]Groupe = ipsec, IP = 64.102.156.87, Détection NAT automatique État:Remote endISunder a NAT deviceThis isend is NOT under a NAT device	
Lancez la phase 1.5 (XAUTH) et demandez les informations d'identification de	24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de charge utile de hachage vide 24 août 11:31:03 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, construction de la charge utile de	

l'utilisateur.	hachage qm 24 août 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE ENVOI du message (msgid=fb709d4d) avec charges utiles : HDR + HASH (8) + ATTR (14) + AUCUNE (0) longueur totale : 72	
	========== XAuth - Demande d'informations d'identification ==========>	
	53511:28:30.43008/24/12Sev=Info/4IKE/0x63000014 REÇU «< ISAKMP OAK TRANS *(HASH, ATTR) à partir de 64.102.156.88 53611:28:30.43108/24/12Sev=Décodage/11IKE/0x63000001 En-tête ISAKMP Initiateur COOKIE : D56197780D7BE3E5 COOKIE du répondeur :1B301D2DE710EDA0 Charge utile suivante : hachage Ver (Hex) : 10 Type d'échange : transaction Indicateurs : (Cryptage) MessageID(hexadécimal) : FB709D4D Longueur : 76 Hachage de données utiles Charge utile suivante : Attributs Réservé: 00 Longueur de la charge utile : 24 Données (en hexadécimal) : C779D5CBC5C75E3576C478A15A7CAB8A83A232D0 Attributs de données utiles Charge utile suivante : Aucune Réservé: 00 Longueur de la charge utile : 20 type : ISAKMP_CFG_REQUEST Réservé: 00 Identifiant: 0000 Type XAUTH : Générique Nom d'utilisateur XAUTH : (vide) Mot de passe utilisateur XAUTH : (vide) 53711:28:30.43108/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState : TM_INITIALEvent : EV_RCVD_MSG	Recevoir la demande d'authentification. La charge utile déchiffrée affiche les champs de nom d'utilisateur et de mot de passe vides.
	53811:28:30.43108/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState : TM_PCS_XAUTH_REQEvent : EV_INIT_XAUTH 53911:28:30.43108/24/12 Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState : TM_PCS_XAUTH_REQEvent : EV_START_RETRY_TMR 54011:28:30.43208/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState :	Lancer la phase 1.5 (XAUTH). Lancez le minuteur de nouvelle tentative en attendant l'entrée de l'utilisateur. Lorsque le minuteur de nouvelle tentative est

	TM_WAIT_4USEREvent : EV_NO_EVENT 541 11:28:36.41508/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState : TM_WAIT_4USEREvent : EV_RCVD_USER_INPUT	épuisé, la connexion est automatiquement déconnectée.
	54211:28:36.41508/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState : TM_WAIT_4USEREvent : EV_SND_MSG 54311:28:36.41508/24/12Sev=Info/4IKE/0x63000013 ENVOI »> ISAKMP OAK TRANS *(HASH, ATTR) à 64.102.156.88 5411:28:36.41508/24/12Sev=Décodage/11IKE/0x63000001 En-tête ISAKMP Initiateur COOKIE : D56197780D7BE3E5 COOKIE du répondeur :1B301D2DE710EDA0 Charge utile suivante : hachage Ver (Hex) : 10 Type d'échange : transaction Indicateurs : (Cryptage) MessageID(hexadécimal) : FB709D4D Longueur : 85 Hachage de données utiles Charge utile suivante : Attributs Réservé: 00 Longueur de la charge utile : 24 Données (en hexadécimal) : 1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5 Attributs de données utiles Charge utile suivante : Aucune Réservé: 00 Longueur de la charge utile : 33 type : ISAKMP_CFG_REPLY Réservé: 00 Identifiant: 0000 Type XAUTH : Générique Nom d'utilisateur XAUTH : (données non affichées) Mot de passe utilisateur XAUTH : (données non affichées)	Une fois l'entrée utilisateur reçue, envoyez les informations d'identification de l'utilisateur au serveur. La charge utile déchiffrée affiche les champs de nom d'utilisateur et de mot de passe remplis (mais masqués). Envoyer la demande de configuration du mode (divers attributs).
	<========== Xauth - Informations d'identification de l'utilisateur ==========	
Recevoir les informations d'identification de l'utilisateur.	24 août 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=fb709d4d) avec charges utiles : HDR + HASH (8) + ATTR (14) + AUCUN (0) longueur totale : 85 24 août 11:31:09 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, process_attr() : Saisissez !	
Traiter les informations d'identification de l'utilisateur. Vérifiez	24 août 11:31:09 [IKEv1 DEBUG]Groupe = ipsec, IP = 64.102.156.87, Traitement des attributs de réponse MODE_CFG. 24 août 11:31:09 [IKEv1 DEBUG]Group = ipsec,	

les informations d'identification et générez la charge utile de configuration du mode.
Configuration appropriée :
 	
`username cisco`
`password cisco`
	Username = user1, IP = 64.102.156.87, IKEGetUserAttributes : DNS principal = 192.168.1.99
	24 août 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes : DNS secondaire = effacé
	24 août 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes : WINS principal = effacé
	24 août 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes : WINS secondaire = effacé
	24 août 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes : split tunneling list = split
	24 août 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes : domaine par défaut = jyoung-labdomain.cisco.com
	24 août 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes : Compression IP = désactivée
	24 août 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes : Politique de fractionnement en canaux = Désactivée
	24 août 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes : Paramètre du proxy du navigateur = pas de modification
	24 août 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes : Contournement du proxy du navigateur local = désactiver
	24 août 11:31:09 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, Utilisateur (user1) authentifié.	

Envoyer le résultat xuath.	24 août 11:31:09 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, construction de données utiles de hachage vierges 24 août 11:31:09 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, construction de la charge utile de hachage qm 24 août 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE ENVOI du message (msgid=5b6910ff) avec charges utiles : HDR + HASH (8) + ATTR (14) + AUCUNE (0) longueur totale : 64	
	========== XAuth - Résultat de l'autorisation ==========>	
	54511:28:36.41608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState : TM_XAUTHREQ_DONEEvent : EV_XAUTHREQ_DOSSIER	Recevez les résultats de l'authentification et les résultats du processus.

	54611:28:36.41608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState : TM_XAUTHREQ_DONEEvent : EV_NO_EVENT 54711:28:36.42408/24/12Sev=Info/5IKE/0x6300002F Paquet ISAKMP reçu : homologue = 64.102.156.88 54811:28:36.42408/24/12Sev=Info/4IKE/0x63000014 REÇU «< ISAKMP OAK TRANS *(HASH, ATTR) à partir de 64.102.156.88 54911:28:36.42508/24/12Sev=Décodage/11IKE/0x63000001 En-tête ISAKMP Initiateur COOKIE : D56197780D7BE3E5 COOKIE du répondeur :1B301D2DE710EDA0 Charge utile suivante : hachage Ver (Hex) : 10 Type d'échange : transaction Indicateurs : (Cryptage) MessageID (hexadécimal) : 5B6910FF Longueur : 76 Hachage de données utiles Charge utile suivante : Attributs Réservé: 00 Longueur de la charge utile : 24 Données (en hexadécimal) : 7DCF47827164198731639BFB7595F694C9DFE85 Attributs de données utiles Charge utile suivante : Aucune Réservé: 00 Longueur de la charge utile : 12 type : ISAKMP_CFG_SET Réservé: 00 Identifiant: 0000 État XAUTH : Passe 55011:28:36.42508/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState : TM_INITIALEvent : EV_RCVD_MSG 55111:28:36.42508/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState : TM_PCS_XAUTH_SETEvent : EV_INIT_XAUTH 55211:28:36.42508/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState : TM_PCS_XAUTH_SETEvent : EV_CHK_AUTH_RESULT	
	55311:28:36.42508/24/12Sev=Info/4IKE/0x63000013 ENVOI »> ISAKMP OAK TRANS *(HASH, ATTR) à 64.102.156.88	Résultat ACK.
	<========== Xauth - Accusé de réception ==========	
Réception et	24 août 11:31:09 [IKEv1]IP = 64.102.156.87,	

traitement de l'ACK ; aucune réponse du serveur.	IKE_DECODE RECEIVED Message (msgid=5b6910ff) avec charges utiles : HDR + HASH (8) + ATTR (14) + AUCUNE (0) longueur totale : 60 24 août 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, process_attr() : Saisissez ! 24 août 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Traitement des attributs ACK cfg	
	5511:28:36.42608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState : TM_XAUTH_DONEEvent : SUC_SUD_DONE_EV_XAUTH 55611:28:36.42608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=5B6910FFCurState : TM_XAUTH_DONEEvent : EV_NO_EVENT 55711:28:36.42608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState : TM_XAUTHREQ_DONEEvent : DEMANDE_TERME_EV 55811:28:36.42608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState : TM_FREEEvent : SUPPRIMER_EV 55911:28:36.42608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState : TM_FREEEvent : EV_NO_EVENT 56011:28:36.42608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : CMN_XAUTH_PROGEvent : SUC_SUD_DONE_EV_XAUTH 56111:28:38.40608/24/12Sev=Débogage/8IKE/0x63000 04C Début du compteur DPD pour IKE SA (I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0) sa->state = 1, sa->dpd.inquif_freq(mSec) = 5000 56211:28:38.40608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : CMN_MODECFG_PROGEvent : EV_INIT_MODECFG 56311:28:38.40608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : CMN_MODECFG_PROGEvent : EV_NO_EVENT	Générer une demande de configuration de mode. La charge utile déchiffrée affiche les paramètres demandés à partir du serveur.

	56411:28:38.40608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState : TM_INITIALEvent : EV_INIT_MODECFG 56511:28:38.40808/24/12Sev=Info/5IKE/0x6300005E Client envoyant une demande de pare-feu au concentrateur 56611:28:38.40908/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState : TM_SND_MODECFGREQEvent : EV_START_RETRY_TMR	
	56711:28:38.40908/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState : TM_SND_MODECFGREQEvent : EV_SND_MSG 56811:28:38.40908/24/12Sev=Info/4IKE/0x63000013 ENVOI »> ISAKMP OAK TRANS *(HASH, ATTR) à 64.102.156.88 56911:28:38.62708/24/12Sev=Décodage/11IKE/0x63000001 En-tête ISAKMP Initiateur COOKIE : D56197780D7BE3E5 COOKIE du répondeur :1B301D2DE710EDA0 Charge utile suivante : hachage Ver (Hex) : 10 Type d'échange : transaction Indicateurs : (Cryptage) MessageID(hexadécimal) : 84B4B653 Longueur : 183 Hachage de données utiles Charge utile suivante : Attributs Réservé: 00 Longueur de la charge utile : 24 Données (en hexadécimal) : 81BFBF6721A744A815D69A315EF4AAA571D6B687 Attributs de données utiles Charge utile suivante : Aucune Réservé: 00 Longueur de la charge utile : 131 type : ISAKMP_CFG_REQUEST Réservé: 00 Identifiant: 0000 Adresse IPv4 : (vide) Masque de réseau IPv4 : (vide) DNS IPv4 : (vide) NBNS IPv4 (WINS) : (vide) Expiration de l'adresse : (vide) Extension Cisco : Bannière : (vide) Extension Cisco : Enregistrer PWD : (vide) Extension Cisco : Nom de domaine par défaut : (vide)	Envoyer la requête mode-config.

	Extension Cisco : Comprend : (vide) Extension Cisco : Nom DNS fractionné : (vide) Extension Cisco : Effectuer PFS : (vide) Inconnu : (vide) Extension Cisco : Serveurs de sauvegarde : (vide) Extension Cisco : Déconnexion de la carte à puce : (vide) Version de l'application : Client VPN Cisco Systems 5.0.07.0290:WinNT Extension Cisco : Type de pare-feu : (vide) Extension Cisco : Nom d'hôte DNS dynamique : ATBASU-LABBOX		
	<========== Requête Mode-config ==========		
Réception de la demande de configuration du mode.	24 août 11:31:11 [IKEv1]IP = 64.102.156.87, message IKE_DECODE REÇU (msgid=84b4b653) avec charges utiles : HDR + HASH (8) + ATTR (14) + AUCUNE (0) longueur totale : 183 24 août 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, process_attr() : Saisissez !	57011:28:38.62808/24/12Sev= Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState : TM_WAIT_MODECFGREPLYEvent : EV_NO_EVENT	Attendez la réponse du serveur.
Demande de configuration du mode de traitement. La plupart de ces valeurs sont généralement configurées dans la stratégie de groupe. Cependant, comme le serveur dans cet exemple a une configuration de base, vous ne les voyez pas ici.	24 août 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Traitement des attributs de demande cfg 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande d'adresse IPV4 reçue ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Requête reçue pour le masque de réseau IPV4 ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Requête reçue pour l'adresse du serveur DNS ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG :		

	Requête reçue pour l'adresse du serveur WINS ! 24 août 11:31:11 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, attribut de mode de transaction reçu non pris en charge : 5 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande de bannière reçue ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Réception d'une demande de paramètre Save PW ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue pour le nom de domaine par défaut ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue pour la liste de tunnels fractionnés ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Requête reçue pour le DNS partagé ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Requête reçue pour le paramètre PFS ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Requête reçue pour le paramètre de proxy du navigateur client ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Réception d'une demande de sauvegarde de la liste d'homologues ip-sec ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue pour le paramètre de déconnexion de la carte à puce du client ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue pour la version de l'application ! 24 août 11:31:11 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, Type de client : Version de l'application WinNTClient : 5.0.07.0290 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue pour FWTYPE ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : La demande reçue de nom d'hôte DHCP pour DDNS est la suivante : ATBASU-LABBOX !	
Construisez la réponse mode-config avec toutes les valeurs configurées. Configuration appropriée :	24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = utilisateur1, IP = 64.102.156.87, Adresse IP obtenue (192.168.1.100) avant le lancement de Mode Cfg (XAuth)) 24 août 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Envoi du	

Remarque : dans ce cas, la même adresse IP est toujours attribuée à l'utilisateur. 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	masque de sous-réseau (255.255.255.0) au client distant 24 août 11:31:11 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, Adresse IP privée attribuée 192.168.1.100 à un utilisateur distant 24 août 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, construction de données utiles de hachage vierges 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, build_cfg_set : domaine par défaut = jyoung-labdomain.cisco.com 24 août 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Send Client Browser Proxy Attributes ! 24 août 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Browser Proxy défini sur No-Modify. Les données du proxy du navigateur ne seront PAS incluses dans la réponse mode-cfg 24 août 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Send Cisco Smartcard Removal Disconnect enable ! ! 24 août 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, construction de la charge utile de hachage qm	
Envoyer la réponse mode-config.	24 août 11:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE ENVOI du message (msgid=84b4b653) avec charges utiles : HDR + HASH (8) + ATTR (14) + AUCUNE (0) longueur totale : 215	
	========== Mode-config Réponse ==========>	
	57111:28:38.63808/24/12Sev=Info/5IKE/0x6300002F Paquet ISAKMP reçu : homologue = 64.102.156.88 57211:28:38.63808/24/12Sev=Info/4IKE/0x63000014 REÇU «< ISAKMP OAK TRANS *(HASH, ATTR) à partir de 64.102.156.88 57311:28:38.63908/24/12Sev=Décodage/11IKE/0x63000001 En-tête ISAKMP Initiateur COOKIE : D56197780D7BE3E5 COOKIE du répondeur :1B301D2DE710EDA0 Charge utile suivante : hachage Ver (Hex) : 10 Type d'échange : transaction Indicateurs : (Cryptage) MessageID(hexadécimal) : 84B4B653 Longueur : 220 Hachage de données utiles Charge utile suivante : Attributs Réservé: 00 Longueur de la charge utile : 24 Données (en hexadécimal) : 6DE2E70ACF6B1858846BC62E590C00A66745D14D	Recevez les valeurs des paramètres mode-config du serveur.

	Attributs de données utiles Charge utile suivante : Aucune Réservé: 00 Longueur de la charge utile : 163 type : ISAKMP_CFG_REPLY Réservé: 00 Identifiant: 0000 Adresse IPv4 : 192.168.1.100 Masque de réseau IPv4 : 255.255.255.0 DNS IPv4 : 192.168.1.99 Extension Cisco : Enregistrer PWD : Non Extension Cisco : Nom de domaine par défaut : jyoungta-labdomain.cisco.com Extension Cisco : Effectuer PFS : Non Version de l'application : Cisco Systems, Inc ASA5505 Version 8.4(4)1, construit par des constructeurs le 14 juin 2012 à 11 h 20 Extension Cisco : Déconnexion de la carte à puce : Oui		
La phase 1 est terminée sur le serveur. Lancer le processus de mode rapide (QM).	24 août 11:31:13 [IKEv1 DECODE]IP = 64.102.156.87, IKE Responder démarrant QM : msg id = 0e83792e 24 août 11:31:13 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, Délai de traitement en mode rapide, DSID Cert/Trans Exch/RM en cours 24 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, protocole ARP gratuit envoyé pour 192.168.1.100 24 août 11:31:13 [IKEv1	57411:28:38.63908/24/12Sev= Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState : TM_WAIT_MODECFGREPLYEvent : EV_RCVD_MSG 57511:28:38.63908/24/12Sev= Info/5IKE/0x63000010 MODE_CFG_REPLY : Attribut = INTERNAL_IPV4_ADDRESS :, valeur = 192.168.1.100 57611:28:38.63908/24/12Sev=Info/5IKE/0x63000010 MODE_CFG_REPLY : Attribut = INTERNAL_IPV4_NETMASK :, valeur = 255.255.255.0 57711:28:38.63908/24/12Sev= Info/5IKE/0x63000010 MODE_CFG_REPLY : Attribut = INTERNAL_IPV4_DNS(1) : , valeur = 192.168.1.99 57811:28:38.63908/24/12Sev=Info/5IKE/0x6300000D MODE_CFG_REPLY : Attribut = MODECFG_UNITY_SAVEPWD : , valeur = 0x00000000 57911:28:38.63908/24/12Sev=Info/5IKE/0x630000E MODE_CFG_REPLY : Attribut = MODECFG_UNITY_DEFDOMAIN : , valeur = jyoung-labdomain.cisco.com 58011:28:38.63908/24/12Sev= Info/5IKE/0x6300000D MODE_CFG_REPLY : Attribut =	Traitez les paramètres et configurez-vous en conséquence.

	DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Reprend Quick Mode Processing, Cert/Trans Exch/RM DSID terminé 24 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, PHASE 1 TERMINÉE	MODECFG_UNITY_PFS : , valeur = 0x00000000 58111:28:38.63908/24/12Sev=Info/5IKE/0x6300000E MODE_CFG_REPLY : Attribut = APPLICATION_VERSION, valeur = Cisco Systems, Inc ASA5505 version 8.4(4)1, créée par constructeurs sur Thu 14-juin-12 11:20 58211:28:38.63908/24/12Sev=Info/5IKE/0x6300000D MODE_CFG_REPLY : Attribut = MODECFG_UNITY_SMARTCARD_REMOVAL_DISCONNECT : , valeur = 0x00000001 58311:28:38.63908/24/12Sev=Info/5IKE/0x6300000D MODE_CFG_REPLY : Attribut = Reçu et utilisation de NAT-T numéro de port , valeur = 0x00001194 58411:28:39.36708/24/12Sev=Débogage/9IKE/0x63000093 La valeur du paramètre ini EnableDNSRedirection est 1 58511:28:39.36708/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState : TM_MODECFG_DONEEvent : SUC_DONE_MODECFG_EV	
Construire et envoyer DPD pour le client.	24 août 11:31:13 [IKEv1]IP = 64.102.156.87, type Keep-alive pour cette connexion : DPD 24 août 11:31:13 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, Démarrage du minuteur de retouche P1 : 82080 secondes. 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, envoi d'un message de notification 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, construction de données utiles de hachage vierges 24 août 11:31:13 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, construction de la charge utile de hachage qm 24 août 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE ENVOI du message (msgid=be8f7821) avec charges utiles : HDR + HASH (8) + NOTIFY (11) + AUCUNE (0) longueur totale : 92		
	========== DPD (Dead Peer Detection) ==========>		
	58811:28:39.79508/24/12Sev=Débogage/7IKE/0x63000015 intf_data&colon ; lcl=0x0501A8C0, mask=0x00FFFFF,	Lancer QM, Phase 2. Construisez	

	bcast=0xFF01A8C0, bcast_vra=0xFF07070A 58911:28:39.79508/24/12Sev=Débogage/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 Réception d'une demande de clé du pilote : IP local = 192.168.1.100, IP GW = 64.102.156.88, IP distant = 0.0.0.0 59111:28:39.79508/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->SA : I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : CMN_ACTIVEEvent : EV_NO_EVENT 59211:28:39.79508/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->QM : MsgID=0E83792ECurState : QM_INITIALEvent : EV_INITIATEUR 59311:28:39.79508/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->QM : MsgID=0E83792ECurState : QM_BLD_MSG1Événement : EV_CHK_PFS 59411:28:39.79608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->QM : MsgID=0E83792ECurState : QM_BLD_MSG1Événement : EV_BLD_MSG 59511:28:39.79608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->QM : MsgID=0E83792ECurState : QM_SND_MSG1Événement : EV_START_RETRY_TMR	QM1. Ce processus comprend : - Hachage - SA avec toutes les propositions de phase 2 prises en charge par le client, le type de tunnel et le cryptage - Nonce - ID client - ID de proxy
	59611:28:39.79608/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->QM : MsgID=0E83792ECurState : QM_SND_MSG1Événement : EV_SND_MSG 59711:28:39.79608/24/12Sev=Info/4IKE/0x63000013 ENVOI » ISAKMP OAK QM *(HASH, SA, NON, ID, ID) à 64.102.156.88	Envoyez QM1.
	<========== Message en mode rapide 1 (QM1) ==========	
Recevez QM1.	24 août 11:31:13 [IKEv1]IP = 64.102.156.87, message reçu IKE_DECODE (msgid=e83792e) avec charges utiles : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + AUCUNE (0) longueur totale : 1026	
Traiter QM1. Configuration appropriée : `crypto dynamic-map DYN 10 set transform-set TRA`	24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, traitement de la charge utile de hachage 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, traitement de la charge utile SA 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, traitement de la	

	charge utile nonce 24 août 11:31:13 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, charge utile d'ID de traitement 24 août 11:31:13 [IKEv1 DECODE]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, ID_IPV4_ADDR ID reçu 192.168.1.100 24 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, Données hôtes proxy distantes reçues dans ID Payload:Adresse 192.168.1.100, Protocole 0, Port 0 24 août 11:31:13 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, charge utile d'ID de traitement 24 août 11:31:13 [IKEv1 DECODE]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, ID_IPV4_ADDR_SUBNET ID reçu—0.0.0—0.0.0.0 24 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = utilisateur1, IP = 64.102.156.87, Données de sous-réseau IP locales reçues dans ID Payload : Adresse 0.0.0.0, Masque 0.0.0, Protocole 0, Port 0 24 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, QM IsRekeyed old n'a pas été trouvé par adresse 24 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, Vérification de la carte de chiffrement statique, vérification de la carte = out-map, seq = 10... 24 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, Vérification de la carte de chiffrement statique contournée : Entrée de carte de chiffrement incomplète ! 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, sélection uniquement des modes UDP-Encapsulated-Tunnel et UDP-Encapsulated-Transport définis par NAT-Traversal 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, sélection uniquement des modes UDP-Encapsulated-Tunnel et UDP-Encapsulated-Transport définis par NAT-Traversal 24 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, homologue distant IKE configuré pour la carte de chiffrement : out-dyn-map 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, traitement de la charge utile IPSec SA	
Construisez QM2. Configuration appropriée : `tunnel-group EZ`	24 août 11:31:13 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = utilisateur1, IP = 64.102.156.87, proposition d'association de sécurité IPSec n° 12, transformation n° 1 acceptableCorrespondances globales entrée d'association de sécurité IPSec n° 10	

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 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, IKE : demande SPI IPSEC : Nouvelle SA embryonnaire créée @ 0xcfdffc90, SCB : 0xCFDFB58, direction : entrant SPI : 0x9E18ACB2 ID de session : 0x00138000 Numéro VPIF : 0x0000004 Type de tunnel : ra Protocole : esp Durée de vie : 240 secondes 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE a obtenu SPI du moteur de clé : SPI = 0x9e18acb2 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, oakley construisant le mode rapide 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, construction de données utiles de hachage vierges 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, construction de la charge utile IPSec SA 24 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, remplacement de la durée de reprise IPSec de l'initiateur de 2147483 à 86400 secondes 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, construction de données utiles IPSec nonce 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, construction de l'ID proxy 24 août 11:31:13 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, ID de proxy de transmission : Hôte distant : 192.168.1.100Protocole 0Port 0 Sous-réseau local :0.0.0.0mask 0.0.0.0 Protocole 0Port 0 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, envoi de la notification RESPONDER LIFETIME à l'initiateur 24 août 11:31:13 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, construction de la charge utile de hachage qm	
Envoyez QM2.	24 août 11:31:13 [IKEv1 DECODE]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, IKE Responder envoyant 2e paquet QM : msg id = 0e83792e 24 août 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE ENVOI du message (msgid=e83792e) avec charges utiles : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE	

	(0) longueur totale : 184	
	========== Message en mode rapide 2 (QM2) ==========>	
	60811:28:39.96208/24/12Sev=Info/4IKE/0x63000014 REÇU «< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFIER : STATUS_RESP_LIFETIME) à partir de 64.102.156.88	Recevez QM2.
	60911:28:39.96408/24/12Sev=Décodage/11IKE/0x63000001 En-tête ISAKMP Initiateur COOKIE : D56197780D7BE3E5 COOKIE du répondeur :1B301D2DE710EDA0 Charge utile suivante : hachage Ver (Hex) : 10 Type d'échange : mode rapide Indicateurs : (Cryptage) MessageID(hexadécimal) : E83792E Longueur : 188 Hachage de données utiles Charge utile suivante : Association de sécurité Réservé: 00 Longueur de la charge utile : 24 Données (en hexadécimal) : CABF38A62C9B88D1691E81F3857D6189534B2EC0 Association de sécurité des données utiles Charge utile suivante : Nuit Réservé: 00 Longueur de la charge utile : 52 DOI : IPsec Situation : (SIT_IDENTITY_ONLY) Proposition de données utiles Charge utile suivante : Aucune Réservé: 00 Longueur de la charge utile : 40 Proposition n° : 1 ID de protocole : PROTO_IPSEC_ESP Taille SPI : 4 Nombre de transformations : 1 SPI : 9E18ACB2 Transformation de charge utile Charge utile suivante : Aucune Réservé: 00 Longueur de la charge utile : 28 N° de transformation : 1 Transform-Id : ESP_3DES Réservé2 : 0000 Type de vie : Secondes Durée de vie (hexadécimale) : 0020C49B Mode d'encapsulation : Tunnel UDP Algorithme d'authentification : SHA1 Nom de charge utile	Traiter QM2. La charge utile déchiffrée affiche les propositions sélectionnées.

	Charge utile suivante : Identification Réservé: 00 Longueur de la charge utile : 24 Données (en hexadécimal) : 3A079B75DA512473706F235EA3FCA61F1D15D4CD Identification des données utiles Charge utile suivante : Identification Réservé: 00 Longueur de la charge utile : 12 Type d'ID : Adresse IPv4 ID de protocole (UDP/TCP, etc.) : 0 Port : 0 Données d'ID&colon ; 192.168.1.100 Identification des données utiles Charge utile suivante : Notification Réservé: 00 Longueur de la charge utile : 16 Type d'ID : Sous-réseau IPv4 ID de protocole (UDP/TCP, etc.) : 0 Port : 0 Données d'ID&colon ; 0.0.0.0/0.0.0.0 Notification de charge utile Charge utile suivante : Aucune Réservé: 00 Longueur de la charge utile : 28 DOI : IPsec ID de protocole : PROTO_IPSEC_ESP Taille Spi : 4 Type de notification : ÉTAT_RESP_LIFETIME SPI : 9E18ACB2 Données et deux-points ; Type de vie : Secondes Durée de vie (hexadécimale) : 00015180	
	61011:28:39.96508/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->QM : MsgID=0E83792ECurState : QM_WAIT_MSG2Event : EV_RCVD_MSG 61111:28:39.96508/24/12Sev=Info/5IKE/0x63000045 La valeur de la notification RESPONDER-LIFETIME est de 86 400 secondes. 61211:28:39.96508/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->QM : MsgID=0E83792ECurState : QM_WAIT_MSG2Event : EV_CHK_PFS 61311:28:39.96508/24/12Sev=Débogage/7IKE/0x63000076	Traiter QM2.
	NAV Trace->QM : MsgID=0E83792ECurState : QM_BLD_MSG3Événement : EV_BLD_MSG 61411:28:39.96508/24/12Sev=Débogage/7IKE/0x63000076 En-tête ISAKMP Initiateur COOKIE : D56197780D7BE3E5 COOKIE du répondeur :1B301D2DE710EDA0	Construisez QM3. Charge utile déchiffrée pour QM3 indiquée ici. Ce processus inclut le hachage.

	Charge utile suivante : hachage Ver (Hex) : 10 Type d'échange : mode rapide Indicateurs : (Cryptage) MessageID(hexadécimal) : E83792E Longueur : 52 Hachage de données utiles Charge utile suivante : Aucune Réservé: 00 Longueur de la charge utile : 24 Données (en hexadécimal) : CDDC20D91EB4B568C826D6A5770A5CF020141236	
	61511:28:39.96508/24/12Sev=Débogage/7IKE/0x63000076 NAV Trace->QM : MsgID=0E83792ECurState : QM_SND_MSG3Événement : EV_SND_MSG 61611:28:39.96508/24/12Sev=Info/4IKE/0x63000013 ENVOI » ISAKMP OAK QM *(HASH) à 64.102.156.88	Envoyez QM3. Le client est maintenant prêt à chiffrer et déchiffrer.
	<========== Message en mode rapide 3 (QM3) ==========	
Recevez QM3.	24 août 11:31:13 [IKEv1]IP = 64.102.156.87, message reçu IKE_DECODE (msgid=e83792e) avec charges utiles : HDR + HASH (8) + AUCUNE (0) longueur totale : 52	

Traiter QM3. Créez les index de paramètres de sécurité entrants et sortants (SPI). Ajoutez une route statique pour l'hôte. Configuration appropriée :
 	
`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 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, traitement de la charge utile de hachage
	24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, chargement de toutes les SA IPSEC
	24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Generating Quick Mode Key !
	24 août 11:31:13 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, règle de chiffrement NP recherchez crypto map out-dyn-map 10 correspondant ACL Inconnu : retourné cs_id=cc107410 ; règle=00000000
	24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Generating Quick Mode Key !
	IPSEC : Nouvelle SA embryonnaire créée @ 0xccc9ed60,
	SCB : 0xCF7F59E0,
	Direction : sortant
	SPI : 0C055290A
	ID de session : 0x00138000
	Numéro VPIF : 0x0000004
	Type de tunnel : ra
	Protocole : esp
	Durée de vie : 240 secondes
	IPSEC : Mise à jour OBSA de l'hôte terminée, SPI	

	0xC055290A IPSEC : Création d'un contexte VPN sortant, SPI 0xC055290A Indicatifs: 0x0000025 SA : 0xccc9ed60 SPI : 0C055290A MTU : 1500 bytes VCID : 0x00000000 Homologue : 0x00000000 SCB : 0xA5922B6B Canal: 0xc82afb60 IPSEC : Contexte VPN sortant terminé, SPI 0xC055290A Handle VPN : 0x0015909c IPSEC : Nouvelle règle de chiffrement sortante, SPI 0xC055290A Adresse Src : 0.0.0.0 Masque Src : 0.0.0.0 Adresse Dst : 192.168.1.100 Masque d'hôte : 255.255.255.255 Ports Src Supérieur : 0 Inférieur : 0 Op: ignorer Ports Dst Supérieur : 0 Inférieur : 0 Op: ignorer Protocole : 0 Utiliser le protocole : faux SPI : 0x00000000 Utiliser SPI : faux IPSEC : Règle de chiffrement sortant terminée, SPI 0xC055290A ID de règle : 0xcb47a710 IPSEC : Nouvelle règle d'autorisation sortante, SPI 0xC055290A Adresse Src : 64.102.156.88 Masque Src : 255.255.255.255 Adresse Dst : 64.102.156.87 Masque d'hôte : 255.255.255.255 Ports Src Supérieur : 4500 Inférieur : 4500 Op: égal Ports Dst Supérieur : 58506 Inférieur : 58506 Op: égal Protocole : 17 Utiliser le protocole : vrai SPI : 0x00000000 Utiliser SPI : faux	

	IPSEC : Règle d'autorisation sortante terminée, SPI 0xC055290A ID de règle : 0xcdf3cfa0 24 août 11:31:13 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, règle de chiffrement NP recherchez crypto map out-dyn-map 10 correspondant ACL Inconnu : retourné cs_id=cc107410 ; règle=00000000 24 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = utilisateur1, IP = 64.102.156.87, Négociation de sécurité terminée pour l'utilisateur (utilisateur1)Répondeur, SPI entrant = 0x9e18acb2, Sortant SPI = 0xc055290a 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE a obtenu un message KEY_ADD pour SA : SPI = 0xc055290a IPSEC : Mise à jour IBSA de l'hôte terminée, SPI 0x9E18ACB2 IPSEC : Création du contexte VPN entrant, SPI 0x9E18ACB2 Indicatifs: 0x0000026 SA : 0xcfdffc90 SPI : 0x9E18ACB2 MTU : 0 bytes VCID : 0x00000000 Homologue : 0x0015909C SCB : 0xA5672481 Canal: 0xc82afb60 IPSEC : Contexte VPN entrant terminé, SPI 0x9E18ACB2 Handle VPN : 0x0016219c IPSEC : Mise à jour du contexte VPN sortant 0x0015909C, SPI 0xC055290A Indicatifs: 0x0000025 SA : 0xccc9ed60 SPI : 0C055290A MTU : 1500 bytes VCID : 0x00000000 Homologue : 0x0016219C SCB : 0xA5922B6B Canal: 0xc82afb60 IPSEC : Contexte VPN sortant terminé, SPI 0xC055290A Handle VPN : 0x0015909c IPSEC : Règle interne sortante terminée, SPI 0xC055290A ID de règle : 0xcb47a710 IPSEC : Règle SPD externe sortante terminée, SPI 0xC055290A ID de règle : 0xcdf3cfa0 IPSEC : Nouvelle règle de flux de tunnel entrant, SPI	

	0x9E18ACB2 Adresse Src : 192.168.1.100 Masque Src : 255.255.255.255 Adresse Dst : 0.0.0.0 Masque d'hôte : 0.0.0.0 Ports Src Supérieur : 0 Inférieur : 0 Op: ignorer Ports Dst Supérieur : 0 Inférieur : 0 Op: ignorer Protocole : 0 Utiliser le protocole : faux SPI : 0x00000000 Utiliser SPI : faux IPSEC : Règle de flux de tunnel entrant terminée, SPI 0x9E18ACB2 ID de règle : 0xcdf15270 IPSEC : Nouvelle règle de déchiffrement entrant, SPI 0x9E18ACB2 Adresse Src : 64.102.156.87 Masque Src : 255.255.255.255 Adresse Dst : 64.102.156.88 Masque d'hôte : 255.255.255.255 Ports Src Supérieur : 58506 Inférieur : 58506 Op: égal Ports Dst Supérieur : 4500 Inférieur : 4500 Op: égal Protocole : 17 Utiliser le protocole : vrai SPI : 0x00000000 Utiliser SPI : faux IPSEC : Règle de déchiffrement entrant terminée, SPI 0x9E18ACB2 ID de règle : 0xce03c2f8 IPSEC : Nouvelle règle d'autorisation entrante, SPI 0x9E18ACB2 Adresse Src : 64.102.156.87 Masque Src : 255.255.255.255 Adresse Dst : 64.102.156.88 Masque d'hôte : 255.255.255.255 Ports Src Supérieur : 58506 Inférieur : 58506 Op: égal Ports Dst Supérieur : 4500	

	Inférieur : 4500 Op: égal Protocole : 17 Utiliser le protocole : vrai SPI : 0x00000000 Utiliser SPI : faux IPSEC : Règle d'autorisation entrante terminée, SPI 0x9E18ACB2 ID de règle : 0xcf6f58c0 24 août 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Pitcher : KEY_UPDATE reçu, spi 0x9e18acb2 24 août 11:31:13 [IKEv1 DEBUG]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, Démarrage du minuteur de retouche P2 : 82080 secondes. 24 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, Ajout d'une route statique pour l'adresse du client : 192.168.1.100	
Phase 2 terminée. Les deux parties chiffrent et déchiffrent maintenant.	24 août 11:31:13 [IKEv1]Groupe = ipsec, Nom d'utilisateur = user1, IP = 64.102.156.87, PHASE 2 TERMINÉE (msgid=0e83792e)	
Pour les clients matériels, un message supplémentaire est reçu où le client envoie des informations sur lui-même. Si vous examinez attentivement, vous devriez trouver le nom d'hôte du client EzVPN, le logiciel exécuté sur le client, ainsi que l'emplacement et le nom du logiciel	24 août 11:31:13 [IKEv1] : IP = 10.48.66.23, message IKE_DECODE RECEIVED (msgid=91facca9) avec charges utiles : HDR + HASH (8) + NOTIFY (11) + AUCUNE (0) longueur totale : 184 24 août 11:31:13 [DEBUG IKEv1] : Groupe = EZ, Nom d'utilisateur = cisco, IP = 10.48.66.23, traitement de la charge utile de hachage 24 août 11:31:13 [DEBUG IKEv1] : Groupe = EZ, Nom d'utilisateur = cisco, IP = 10.48.66.23, charge utile de notification de traitement 24 août 11:31:13 [DÉCODE IKEv1] : DESCRIPTEUR OBSOLÈTE - INDEX 1 24 août 11:31:13 [DÉCODE IKEv1] : 0000: 0000000 7534000B 62736E73 2D383731 ....u4.**bsns-871** 0010: 2D332E75 32000943 6973636F 20383731 **-3**.u2..**Cisco 871** 0020: 7535000B 46484B30 39343431 32513675 u5..FHK094412Q6u 0030: 36000932 32383538 39353638 75390009 6..228589568u9. 0040: 31343532 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 août 11:31:13 [DEBUG IKEv1] : Groupe = EZ, Nom d'utilisateur = cisco, IP = 10.48.66.23, Traitement du hachage PSK 24 août 11:31:13 [IKEv1] : Groupe = EZ, Nom d'utilisateur = cisco, IP = 192.168.1.100, taille de hachage PSK incohérente 24 août 11:31:13 [DEBUG IKEv1] : Groupe = EZ, Nom d'utilisateur = cisco, IP = 10.48.66.23, échec de la vérification du hachage PSK !	

Vérification du tunnel

ISAKMP

La sortie de la commande **sh cry isa sa det** est :

```
 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

Puisque le protocole ICMP (Internet Control Message Protocol) est utilisé pour déclencher le tunnel, une seule SA IPsec est active. Le protocole 1 est ICMP. Notez que les valeurs SPI diffèrent de celles négociées dans les débogages. Il s'agit, en fait, du même tunnel après la retouche de phase 2.

La sortie de la commande **sh crypto ipsec sa** est :

```
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
```

Informations connexes

- Article Wikipedia sur IPsec
- Dépannage IPsec : Présentation et utilisation des commandes de débogage
- Support et documentation techniques - Cisco Systems