

# De la note en tech de debugs ASA IPsec et d'IKE (mode IKEv1 agressif) dépannage

## Contenu

[Introduction](#)

[Principale question](#)

[Scénario](#)

[commandes de débogage utilisées](#)

[Configuration ASA](#)

[Débogage](#)

[Vérification de tunnel](#)

[ISAKMP](#)

[IPsec](#)

[Informations connexes](#)

## Introduction

Ce document décrit met au point sur l'appliance de sécurité adaptable Cisco (ASA) quand le mode agressif et la clé pré-partagée (PSK) sont utilisés. La traduction de certaines lignes de débogage dans la configuration est également abordée. Cisco vous recommande ont une connaissance de base d'IPsec et d'Échange de clés Internet (IKE).

Ce document ne discute pas le dépassement du trafic après que le tunnel ait été établi.

## Principale question

L'IKE et l'IPsec met au point sont parfois cryptiques, mais vous pouvez les employer afin de comprendre des problèmes avec l'établissement de tunnel VPN d'IPsec.

## Scénario

Le mode agressif est typiquement utilisé en cas d'Easy VPN (EzVPN) avec le logiciel (Client VPN Cisco) et les clients matériels (Serveur de sécurité adaptatif dédié de la gamme Cisco ASA 5505 ou Cisco IOS<sup>?</sup> Routeurs de logiciel), mais seulement quand une clé pré-partagée est utilisée. À la différence du mode principal, le mode agressif se compose de trois messages.

Met au point sont d'une ASA qui exécute la version de logiciel 8.3.2 et agit en tant que serveur d'EzVPN. Le client d'EzVPN est un client logiciel.

## commandes de débogage utilisées

Ce sont les commandes de débogage utilisées dans ce document :

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

## Configuration ASA

La configuration ASA dans cet exemple est censée pour être 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

Remarque: Référez-vous aux [informations importantes sur les commandes de débogage](#)

avant d'utiliser les commandes de débogage.

Description de messages serveur	Debugs		Description de message de client
	<p>49711:28:30.28908/24/12Sev=Info/6IKE/0x6300003B Tenter pour établir une connexion avec 64.102.156.88. 49811:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState : AM_INITIALEvent : EV_INITIATOR 49911:28:30.29708/24/12Sev=Info/4IKE/0x63000001 Commencer la négociation de Phase 1 d'IKE 50011:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState : AM_SND_MSG1Event : EV_GEN_DHKEY 50111:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState : AM_SND_MSG1Event : EV_BLD_MSG 50211:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState : AM_SND_MSG1Event : EV_START_RETRY_TMR 50311:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState : AM_SND_MSG1Event : EV_SND_MSG</p>		<p>Débuts agressifs de mode. Élaboration AM1. Ce processus inclut : - ISAKMP HDR - Les dispositifs de sécurité (SA) qui contiennent toute transforment des charges utiles et des propositions prises en charge par le client - Charge utile de Key Exchange - ID de demandeur de Phase 1 - Nonce</p>
	<p>50411:28:30.30408/24/12Sev=Info/4IKE/0x63000013 ENVOYANT CHÊNE AG (SA, KE d'ISAKMP de &gt;&gt;&gt;, NON, ID, VID(Xauth), VID(dpd), VID(Frag), VID (nat-T), VID(Unity)) à 64.102.156.88</p>		<p>Envoyez AM1.</p>
	<p>===== agressif du message 1 de &lt;===== (AM1)</p>		
<p>Recevez AM1 du client.</p>	<p>24 août 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE A REÇU le message (msgid=0) avec des charges utiles : HDR + SA (1) + le KE (4) + NONCE (10) + ID (5) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) +</p>	<p>50611:28:30.33308/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState : AM_WAIT_MSG2Event : EV_NO_EVENT</p>	<p>Attente la réponse du serveur.</p>

	<p>CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + AUCUN (0) longueurs totales : 849</p>		
<p>Processus AM1. Compare a reçu des propositions et les transforme avec ceux déjà configurés pour des correspondances. Configuration appropriée : L'ISAKMP est activé sur l'interface, et au moins une stratégie est définie qui apparie ce que le client a envoyé :</p> <pre>crypto isakmp enable outside crypto isakmp policy 10 authentication pre- share encryption aes hash sha group 2 lifetime 86400</pre> <p>Groupe de tunnels appariant le présent de nom d'identité :</p> <pre>tunnel-group EZ type remote-access tunnel-group EZ general-attributes default-group-policy EZ tunnel-group EZ ipsec- attributes pre-shared-key cisco</pre>	<p>24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, traitant la charge utile SA  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, traitant la charge utile du KE  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, traitant la charge utile ISA_KE  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, traitant la charge utile de nonce  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, charge utile d'IDENTIFICATEUR DE PROCESSUS  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, traitant la charge utile VID  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, Xauth reçu V6 VID  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, traitant la charge utile VID  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, DPD reçu VID  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, traitant la charge utile VID  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, fragmentation reçue VID  24 août le DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, pair d'IKE a inclus des indicateurs de capacité de fragmentation d'IKE : Mode principal : Mode de TrueAggressive : Faux  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, traitant la charge utile VID  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, ver reçu 02 VID de NAT-Traversal  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, traitant la charge utile VID  24 août DEBUG [IKEv1 de 11:31:03] IP = 64.102.156.87, client reçu VID de Cisco Unity  24 août 11:31:03 [IKEv1]IP = 64.102.156.87, connexion a débarqué sur l'ipsec de tunnel_group  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, traitant la charge utile d'IKE SA  24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5  24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5  24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p>		

	<p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août panne de 11:31:03 [IKEv1]Phase 1 : Types mal adaptés d'attribut pour la description de groupe de classe : Rcv'd : Groupe 2Cfg'd : Groupe 5</p> <p>24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, proposition d'IKE SA # 1, transformant de # l'entrée globale d'IKE 5 acceptableMatches # 1</p>	
<p>Élaboration AM2. Ce processus inclut :</p> <ul style="list-style-type: none"> <li>- stratégies choisies</li> <li>- Protocole DH (Diffie-Hellman)</li> <li>- ID de responder</li> <li>- authentique</li> <li>- Charge utile de détection de Traduction</li> </ul>	<p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile de SA ISAKMP</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile du KE</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile de nonce</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, générant des clés pour le responder...</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP</p>	

d'adresses de réseau (NAT)	<p>= 64.102.156.87, construisant la charge utile d'ID</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile d'informations parasites</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, calculant des informations parasites pour l'ISAKMP</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile du Cisco Unity VID</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile du Xauth V6 VID</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile de vid de dpd</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile du ver 02 du NAT-Traversal VID</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile de Nat-détection</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, calculant les informations parasites NAT de détection</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile de Nat-détection</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, calculant les informations parasites NAT de détection</p> <p>24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la fragmentation VID + ont étendu la charge utile de capacités</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile VID</p> <p>24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, envoient Altiga/Cisco VPN3000/Cisco ASA LE gw VID</p>	
Envoyez AM2.	<p>24 août 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE envoyant message (msgid=0) avec des charges utiles : HDR + SA (1) + le KE (4) + NONCE (10) + ID (5) + INFORMATIONS PARASITES (8) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + NAT-D (130) + NAT-D (130) + CONSTRUCTEUR (13) + CONSTRUCTEUR (13) + AUCUN (0) longueurs totales : 444</p>	
	<p>=====&gt; <b>agressif du message 2 de</b>  <b>===== (AM2)</b></p>	
	<p>50711:28:30.40208/24/12Sev=Info/5IKE/0x6300002F  Paquet reçu d'ISAKMP : pair = 64.102.156.8  50811:28:30.40308/24/12Sev=Info/4IKE/0x63000014</p>	Recevez AM2.

	RECEVANT CHÊNE AG (SA d'ISAKMP de <<<, le KE, NON, ID, INFORMATIONS PARASITES, VID(Unity), VID(Xauth), VID(dpd), VID (nat-T), NAT-D, NAT-D, VID(Frag), VID (?) de 64.102.156.88 51011:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_WAIT_MSG2Event : EV_RCVD_MSG	
	51111:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Le pair est un pair conforme de Cisco Unity 51211:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Le pair prend en charge le XAUTH 51311:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Le pair prend en charge DPD 51411:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Le pair prend en charge NAT-T 51511:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Le pair prend en charge des charges utiles de fragmentation d'IKE 51611:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_WAIT_MSG2Event : EV_GEN_SKEYID 51711:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_WAIT_MSG2Event : EV_AUTHENTICATE_PEER 51811:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_WAIT_MSG2Event : EV_ADJUST_PORT 51911:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_WAIT_MSG2Event : EV_CRYPTO_ACTIVE	Processus AM 2.
	52011:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_SND_MSG3Event : EV_BLD_MSG] 52111:28:30.42208/24/12Sev=Debug/8IKE/0x63000001 L'ID Construction de constructeur IOS a commencé 52211:28:30.42208/24/12Sev=Info/6IKE/0x63000001 ID Construction de constructeur IOS réussi	Élaboration AM3. Ce processus inclut le client authentique. En ce moment toutes les données appropriées pour le cryptage ont été déjà permutées.
	52311:28:30.42308/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : AM_SND_MSG3Event : EV_SND_MSG 52411:28:30.42308/24/12Sev=Info/4IKE/0x63000013 ENVOYANT CHÊNE AG D'ISAKMP DE >>> * (LES INFORMATIONS PARASITES, ANNONCENT :	Envoyez AM3.

	STATUS_INITIAL_CONTACT, NAT-D, NAT-D, VID (?), VID(Unity) à 64.102.156.88	
	===== agressif du message 3 de <===== (AM3)	
Recevez AM3 du client.	24 août 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE A REÇU le message (msgid=0) avec des charges utiles : HDR + les INFORMATIONS PARASITES (8) + ANNONCENT (11) + NAT-D (130) + NAT-D (130) + le CONSTRUCTEUR (13) + le CONSTRUCTEUR (13) + AUCUN (0) longueurs totales : 168	
Le processus AM 3. confirment l'utilisation du NAT Traversal (NAT-T). Les deux côtés sont maintenant prêts à commencer le cryptage du trafic.	<p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, traitant la charge utile d'informations parasites</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, calculant des informations parasites pour l'ISAKMP</p> <p>24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, traitant informant la charge utile</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, traitant la charge utile de Nat-détection</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, calculant les informations parasites NAT de détection</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, traitant la charge utile de Nat-détection</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, calculant les informations parasites NAT de détection</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, traitant la charge utile VID</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, traitant la charge utile d'ID de constructeur IOS/PIX (version : 1.0.0, capacités : 00000408)</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, traitant la charge utile VID</p> <p>24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, ont reçu le client VID de Cisco Unity</p> <p>24 août 11:31:03 [IKEv1]Group = ipsec, IP = 64.102.156.87, détection NAT automatique État : L'endISbehind distant un deviceThisend NAT n'est pas derrière un périphérique NAT</p>	
Phase initiée 1.5 (XAUTH), et identifiants utilisateurs de demande.	<p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile vide d'informations parasites</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:03], IP = 64.102.156.87, construisant la charge utile d'informations parasites de qm</p> <p>24 août 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE envoyant message (msgid=fb709d4d) avec des charges utiles : HDR + INFORMATIONS PARASITES</p>	



	(8) + ATTR (14) + AUCUN (0) longueurs totales : 72	
	<b>Xauth de ===== - =====&gt; de demande de qualifications</b>	
	<p>53511:28:30.43008/24/12Sev=Info/4IKE/0x63000014 RECEVANT LE transport de CHÊNE d'ISAKMP de &lt;&lt;&lt; * (INFORMATIONS PARASITES, ATTR) de 64.102.156.88 53611:28:30.43108/24/12Sev=Decode/11IKE/0x63000001 En-tête d'ISAKMP Demandeur COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Prochaine charge utile : Informations parasites Version (Hex):10 Type d'échange : Transaction Indicateurs : (Cryptage) MessageID(Hex):FB709D4D Length:76 Informations parasites de charge utile Prochaine charge utile : Attributs Réservé : 00 Longueur de charge utile : 24 Données (dans l'hexa) : C779D5CBC5C75E3576C478A15A7CAB8A83A232D0 Attributs de charge utile Prochaine charge utile : Aucun Réservé : 00 Longueur de charge utile : 20 Type : ISAKMP_CFG_REQUEST Réservé : 00 Identifiant : 0000 Type de XAUTH : Générique Nom d'utilisateur de XAUTH : (vide) Mot de passe utilisateur de XAUTH : (vide) 53711:28:30.43108/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;TM:MsgID=FB709D4DCurState : TM_INITIALEvent : EV_RCVD_MSG</p>	<p>Recevez la demande d'autorisation. La charge utile déchiffrée affiche les champs vides de nom d'utilisateur et mot de passe.</p>
	<p>53811:28:30.43108/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;TM:MsgID=FB709D4DCurState : TM_PCS_XAUTH_REQEvent : EV_INIT_XAUTH 53911:28:30.43108/24/12 Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;TM:MsgID=FB709D4DCurState : TM_PCS_XAUTH_REQEvent : EV_START_RETRY_TMR 54011:28:30.43208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;TM:MsgID=FB709D4DCurState : TM_WAIT_4USEREvent : EV_NO_EVENT 541 11:28:36.41508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;TM:MsgID=FB709D4DCurState : TM_WAIT_4USEREvent : EV_RCVD_USER_INPUT</p>	<p>Phase initiée 1.5 (XAUTH). Temporisateur initié de relance comme il attend l'entrée d'utilisateur. Quand le temporisateur de relance s'épuise, la connexion est automatiquement déconnectée.</p>
	<p>54211:28:36.41508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;TM:MsgID=FB709D4DCurState : TM_WAIT_4USEREvent : EV_SND_MSG 54311:28:36.41508/24/12Sev=Info/4IKE/0x63000013 ENVOYANT LE transport de CHÊNE d'ISAKMP de &gt;&gt;&gt; *</p>	<p>Une fois que l'entrée d'utilisateur est reçue, envoyez les identifiants</p>

	<p>(INFORMATIONS PARASITES, ATTR) à 64.102.156.88  54411:28:36.41508/24/12Sev=Decode/11IKE/0x63000001  En-tête d'ISAKMP  Demandeur COOKIE:D56197780D7BE3E5  Responder COOKIE:1B301D2DE710EDA0  Prochaine charge utile : Informations parasites  Version (Hex):10  Type d'échange : Transaction  Indicateurs : (Cryptage)  MessageID(Hex):FB709D4D  Length:85  Informations parasites de charge utile  Prochaine charge utile : Attributs  Réservé : 00  Longueur de charge utile : 24  Données (dans l'hexa) :  1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5  Attributs de charge utile  Prochaine charge utile : Aucun  Réservé : 00  Longueur de charge utile : 33  Type : ISAKMP_CFG_REPLY  Réservé : 00  Identifiant : 0000  Type de XAUTH : Générique  Nom d'utilisateur de XAUTH : (données non affichées)  Mot de passe utilisateur de XAUTH : (données non affichées)</p>	<p>utilisateurs au serveur. Les expositions déchiffrées de charge utile ont rempli (mais masqué) champs de nom d'utilisateur et mot de passe. Demande de config de mode d'envoi (divers attributs).</p>
	<p><b>Xauth de &lt;===== - =====</b>  <b>d'identifiants utilisateurs</b></p>	
<p>Recevez les identifiants utilisateurs.</p>	<p>24 août 11:31:09 [IKEv1]IP = 64.102.156.87,  IKE_DECODE A REÇU le message (msgid=fb709d4d)  avec des charges utiles : HDR + INFORMATIONS  PARASITES (8) + ATTR (14) + AUCUN (0)  longueur totale : 85  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09], IP = 64.102.156.87, process_attr() : Entrez !</p>	
<p>Identifiants utilisateurs de processus. Vérifiez les qualifications, et générez la charge utile de configuration de mode.  Configuration appropriée :  username cisco  password cisco</p>	<p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09], IP = 64.102.156.87, traitant des attributs de réponse MODE_CFG.  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09], nom d'utilisateur = user1, IP = 64.102.156.87,  IKEGetUserAttributes : DNS principal = 192.168.1.99  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09], nom d'utilisateur = user1, IP = 64.102.156.87,  IKEGetUserAttributes : DNS secondaire = effacé  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09], nom d'utilisateur = user1, IP = 64.102.156.87,  IKEGetUserAttributes : WINS primaires = effacé  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09], nom d'utilisateur = user1, IP = 64.102.156.87,  IKEGetUserAttributes : WINS secondaires = effacé  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09],</p>	

	<p>nom d'utilisateur = user1, IP = 64.102.156.87,  IKEGetUserAttributes : liste = fractionnement de  Segmentation de tunnel  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09],  nom d'utilisateur = user1, IP = 64.102.156.87,  IKEGetUserAttributes : domaine par défaut = jyoungta-  labdomain.cisco.com  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09],  nom d'utilisateur = user1, IP = 64.102.156.87,  IKEGetUserAttributes : Le compactage IP = a désactivé  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09],  nom d'utilisateur = user1, IP = 64.102.156.87,  IKEGetUserAttributes : La stratégie de Segmentation de  tunnel = a désactivé  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09],  nom d'utilisateur = user1, IP = 64.102.156.87,  IKEGetUserAttributes : Le paramètre de proxy du  navigateur = NO--modifiant  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09],  nom d'utilisateur = user1, IP = 64.102.156.87,  IKEGetUserAttributes : Gens du pays = débranchement de  contournement de navigateur proxy  24 août 11:31:09 [IKEv1]Group = ipsec, nom d'utilisateur =  user1, IP = 64.102.156.87, utilisateur (user1) authentifié.</p>	
<p>Envoyez le résultat de xauth.</p>	<p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09],  nom d'utilisateur = user1, IP = 64.102.156.87, construisant  la charge utile vide d'informations parasites  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09],  nom d'utilisateur = user1, IP = 64.102.156.87, construisant  la charge utile d'informations parasites de qm  24 août 11:31:09 [IKEv1]IP = 64.102.156.87,  IKE_DECODE envoyant message (msgid=5b6910ff) avec  des charges utiles : HDR + INFORMATIONS PARASITES  (8) + ATTR (14) + AUCUN (0) longueurs totales : 64</p>	
	<p><b>Xauth de ===== - =====&gt; de  résultat d'autorisation</b></p>	
	<p>54511:28:36.41608/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;TM:MsgID=FB709D4DCurState :  TM_XAUTHREQ_DONEEvent : EV_XAUTHREQ_DONE  54611:28:36.41608/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;TM:MsgID=FB709D4DCurState :  TM_XAUTHREQ_DONEEvent : EV_NO_EVENT  54711:28:36.42408/24/12Sev=Info/5IKE/0x6300002F  Paquet reçu d'ISAKMP : pair = 64.102.156.88  54811:28:36.42408/24/12Sev=Info/4IKE/0x63000014  RECEVANT LE transport de CHÊNE d'ISAKMP de &lt;&lt;&lt; *  (INFORMATIONS PARASITES, ATTR) de 64.102.156.88  54911:28:36.42508/24/12Sev=Decode/11IKE/0x63000001  En-tête d'ISAKMP  Demandeur COOKIE:D56197780D7BE3E5  Responder COOKIE:1B301D2DE710EDA0  Prochaine charge utile : Informations parasites  Version (Hex):10</p>	<p>Recevez les résultats authentiques, et les résultats de processus.</p>

	<p>Type d'échange : Transaction  Indicateurs : (Cryptage)  MessageID(Hex):5B6910FF  Length:76  Informations parasites de charge utile  Prochaine charge utile : Attributs  Réservé : 00  Longueur de charge utile : 24  Données (dans l'hexa) :  7DCF47827164198731639BFB7595F694C9DDFE85  Attributs de charge utile  Prochaine charge utile : Aucun  Réservé : 00  Longueur de charge utile : 12  Type : ISAKMP_CFG_SET  Réservé : 00  Identifiant : 0000  État de XAUTH : Passez  55011:28:36.42508/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;TM:MsgID=5B6910FFCurState :  TM_INITIALEvent : EV_RCVD_MSG  55111:28:36.42508/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;TM:MsgID=5B6910FFCurState :  TM_PCS_XAUTH_SETEvent : EV_INIT_XAUTH  55211:28:36.42508/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;TM:MsgID=5B6910FFCurState :  TM_PCS_XAUTH_SETEvent : EV_CHK_AUTH_RESULT</p>	
	<p>55311:28:36.42508/24/12Sev=Info/4IKE/0x63000013  ENVOYANT LE transport de CHÊNE d'ISAKMP de &gt;&gt;&gt; *  (INFORMATIONS PARASITES, ATTR) à 64.102.156.88</p>	<p>Résultat ACK.</p>
	<p><b>Xauth de &lt;===== - =====  d'accusé de réception</b></p>	
<p>Recevez et traitez l'ACK ; aucune réponse de serveur.</p>	<p>24 août 11:31:09 [IKEv1]IP = 64.102.156.87,  IKE_DECODE A REÇU le message (msgid=5b6910ff)  avec des charges utiles : HDR + INFORMATIONS  PARASITES (8) + ATTR (14) + AUCUN (0) longueurs  totales : 60  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09],  nom d'utilisateur = user1, IP = 64.102.156.87,  process_attr() : Entrez !  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:09],  nom d'utilisateur = user1, IP = 64.102.156.87, traitant des  attributs du cfg ACK</p>	
	<p>55511:28:36.42608/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;TM:MsgID=5B6910FFCurState :  TM_XAUTH_DONEEvent :  EV_XAUTH_DONE_SUC  55611:28:36.42608/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;TM:MsgID=5B6910FFCurState :  TM_XAUTH_DONEEvent : EV_NO_EVENT  55711:28:36.42608/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;TM:MsgID=FB709D4DCurState :  TM_XAUTHREQ_DONEEvent : EV_TERM_REQUEST</p>	<p>Générez la demande de mode-config. Les expositions déchiffrées de charge utile ont demandé des paramètres de serveur.</p>

	<p>55811:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;TM:MsgID=FB709D4DCurState : TM_FREEEvent : EV_REMOVE</p> <p>55911:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;TM:MsgID=FB709D4DCurState : TM_FREEEvent : EV_NO_EVENT</p> <p>56011:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : CMN_XAUTH_PROGEvent : EV_XAUTH_DONE_SUC</p> <p>56111:28:38.40608/24/12Sev=Debug/8IKE/0x6300004C Démarrer le temporisateur DPD pour IKE SA (I_Cookie=D56197780D7BE3E5 ) Sa-&gt;state R_Cookie=1B301D2DE710EDA0 = 1, sa- &gt;dpd.worry_freq(mSec) = 5000</p> <p>56211:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : CMN_MODECFG_PROGEvent : EV_INIT_MODECFG</p> <p>56311:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState : CMN_MODECFG_PROGEvent : EV_NO_EVENT</p> <p>56411:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;TM:MsgID=84B4B653CurState : TM_INITIALEvent : EV_INIT_MODECFG</p> <p>56511:28:38.40808/24/12Sev=Info/5IKE/0x6300005E Client envoyant une demande de Pare-feu au concentrateur</p> <p>56611:28:38.40908/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;TM:MsgID=84B4B653CurState : TM_SND_MODECFGREQEvent : EV_START_RETRY_TMR</p>	
	<p>56711:28:38.40908/24/12Sev=Debug/7IKE/0x63000076 NAV Trace-&gt;TM:MsgID=84B4B653CurState : TM_SND_MODECFGREQEvent : EV_SND_MSG</p> <p>56811:28:38.40908/24/12Sev=Info/4IKE/0x63000013 ENVOYANT LE transport de CHÊNE d'ISAKMP de &gt;&gt;&gt; * (INFORMATIONS PARASITES, ATTR) à 64.102.156.88</p> <p>56911:28:38.62708/24/12Sev=Decode/11IKE/0x63000001 En-tête d'ISAKMP Demandeur COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Prochaine charge utile : Informations parasites Version (Hex):10 Type d'échange : Transaction Indicateurs : (Cryptage) MessageID(Hex):84B4B653 Length:183</p> <p>Informations parasites de charge utile Prochaine charge utile : Attributs Réservé : 00</p>	<p>Envoyez la demande de mode-config.</p>

	<p>Longueur de charge utile : 24  Données (dans l'hexa) :  81BFBF6721A744A815D69A315EF4AAA571D6B687</p> <p>Attributs de charge utile  Prochaine charge utile : Aucun  Réservé : 00  Longueur de charge utile : 131  Type : ISAKMP_CFG_REQUEST  Réservé : 00  Identifiant : 0000  Ipv4 adres : (vide)  Netmask d'ipv4 : (vide)  DN d'ipv4 : (vide)  Ipv4 NBNS (WINS) : (vide)  Échéance d'adresse : (vide)  Extension de Cisco : Bannière : (vide)  Extension de Cisco : Sauvegardez le PWD : (vide)  Extension de Cisco : Nom de domaine par défaut : (vide)  Extension de Cisco : Le fractionnement incluent : (vide)  Extension de Cisco : Nom DNS fendu : (vide)  Extension de Cisco : Faites le PFS : (vide)  Inconnu : (vide)  Extension de Cisco : Serveurs de sauvegarde : (vide)  Extension de Cisco : Débranchement de suppression de Smart Card : (vide)  Version d'application : Client vpn 5.0.07.0290:WinNT de Cisco Systems  Extension de Cisco : Type de Pare-feu : (vide)  Extension de Cisco : Adresse Internet dynamique de DN : ATBASU-LABBOX</p>	
	<p style="text-align: center;">===== de demande de Mode-config de  &lt;=====</p>	
<p>Recevez la demande de mode-config.</p>	<p>24 août 11:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE A REÇU le message (msgid=84b4b653) avec des charges utiles : HDR + INFORMATIONS PARASITES (8) + ATTR (14) + AUCUN (0) longueurs totales : 183  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP =</p>	<p>57011:28:38.62808/24/12Sev= Debug/7IKE/0x63000076  NAV Trace-  &gt;TM:MsgID=84B4B653CurState : TM_WAIT_MODECFGREPLYEvent : EV_NO_EVENT</p> <p>Attente la réponse de serveur.</p>

	64.102.156.87, process_attr() : Entrez !		
<p>Demande de processus de mode-config. Plusieurs de ces valeurs sont habituellement configurées dans la stratégie de groupe. Cependant, puisque le serveur dans cet exemple a très une configuration de base, vous ne les voyez pas ici.</p>	<p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, traitant des attributs de demande de cfg</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue d'ipv4 adres !</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue de masque de réseau d'IPV4 !</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue de l'adresse de serveur de DNS !</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue d'adresse de serveur WINS !</p> <p>24 août 11:31:11 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, a reçu l'attribut non vérifié de mode transaction : 5</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue de bannière !</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue de la configuration picowatt de sauvegarde !</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue du nom de domaine par défaut !</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue de liste de tunnel partagé !</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue des DN fendus !</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue d'établissement de PFS !</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue de paramètre de proxy du navigateur de client !</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, MODE_CFG : Demande reçue de liste de sauvegarde de pair d'IP-sec !</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11],</p>		

	<p>nom d'utilisateur = user1, IP = 64.102.156.87,  MODE_CFG : Demande reçue de la configuration de débranchement de suppression de carte à puce de client !  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11],  nom d'utilisateur = user1, IP = 64.102.156.87,  MODE_CFG : Demande reçue de version d'application !  24 août 11:31:11 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, type de client : Version d'application de WinNTClient : 5.0.07.0290  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11],  nom d'utilisateur = user1, IP = 64.102.156.87,  MODE_CFG : Demande reçue de FWTYPE !  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11],  nom d'utilisateur = user1, IP = 64.102.156.87,  MODE_CFG : La demande reçue de l'adresse Internet DHCP pour DDNS est : ATBASU-LABBOX !</p>	
<p>Construisez la réponse de mode-config avec toutes les valeurs qui sont configurées.  Configuration appropriée :  Notez dans ce cas, l'utilisateur est toujours assigné le même IP.</p> <pre>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</pre>	<p>24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, ont obtenu l'adr IP (192.168.1.100) avant d'initier le mode Cfg (le Xauth activé)  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, envoyant le masque de sous-réseau (255.255.255.0) au client distant  24 août 11:31:11 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, a assigné l'adresse IP privée 192.168.1.100 à l'utilisateur distant  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, construisant la charge utile vide d'informations parasites  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, construct_cfg_set : domaine par défaut = jyoungta-labdomain.cisco.com  24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, envoient des attributs de navigateur proxy de client !  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, positionnement de navigateur proxy NO--à modifier. Des données de navigateur proxy ne seront pas incluses dans la réponse de mode-cfg  24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, envoient l'enable de débranchement de suppression de carte à puce de Cisco !!  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:11], nom d'utilisateur = user1, IP = 64.102.156.87, construisant la charge utile d'informations parasites de qm</p>	
<p>Envoyez la réponse de mode-config.</p>	<p>24 août 11:31:11 [IKEv1]IP = 64.102.156.87,  IKE_DECODE envoyant message (msgid=84b4b653)  avec des charges utiles : HDR + INFORMATIONS  PARASITES (8) + ATTR (14) + AUCUN (0) longueurs  totales : 215</p>	



	=====> de réponse de Mode-config de =====		
	57111:28:38.63808/24/12Sev=Info/5IKE/0x6300002F Paquet reçu d'ISAKMP : pair = 64.102.156.88 57211:28:38.63808/24/12Sev=Info/4IKE/0x63000014 RECEVANT LE transport de CHÊNE d'ISAKMP de <<< * (INFORMATIONS PARASITES, ATTR) de 64.102.156.88 57311:28:38.63908/24/12Sev=Decode/11IKE/0x63000001 En-tête d'ISAKMP Demandeur COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Prochaine charge utile : Informations parasites Version (Hex):10 Type d'échange : Transaction Indicateurs : (Cryptage) MessageID(Hex):84B4B653 Length:220 Informations parasites de charge utile Prochaine charge utile : Attributs Réservé : 00 Longueur de charge utile : 24 Données (dans l'hexa) : 6DE2E70ACF6B1858846BC62E590C00A66745D14D Attributs de charge utile Prochaine charge utile : Aucun Réservé : 00 Longueur de charge utile : 163 Type : ISAKMP_CFG_REPLY Réservé : 00 Identifiant : 0000 Ipv4 adres : 192.168.1.100 Netmask d'ipv4 : 255.255.255.0 DN d'ipv4 : 192.168.1.99 Extension de Cisco : Sauvegardez le PWD : Non Extension de Cisco : Nom de domaine par défaut : jyoungta-labdomain.cisco.com Extension de Cisco : Faites le PFS : Non Version d'application : Version 8.4(4)1 de Cisco Systems, Inc ASA5505 établie par des builders Thu 14-Jun-12 11:20 Extension de Cisco : Débranchement de suppression de Smart Card : Oui		Recevez les valeurs de paramètre de mode-config du serveur.
Le Phase 1 se termine sur le serveur. Processus rapide initié du mode (QM).	24 août 11:31:13 [IKEv1 DÉCODENT] IP = 64.102.156.87, responder d'IKE commençant QM : id de msg = 0e83792e 24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:13], nom	57411:28:38.63908/24/12Sev= Debug/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/5IK	Les paramètres de processus, et se configurent en conséquence.

	<p>d'utilisateur = user1, IP = 64.102.156.87, retardent le mode rapide traitant, le CERT/transport Exch/RM DSID en cours  24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, ARP gratuit envoyé pour 192.168.1.100  24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, reprennent le mode rapide traitant, le CERT/transport Exch/RM DSID terminé  24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, PHASE 1 S'EST TERMINÉ</p>	<p>E/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/0x6300000E  MODE_CFG_REPLY : Attribut = MODECFG_UNITY_DEFDOMAIN : , valeur = jyoungta-labdomain.cisco.com  58011:28:38.63908/24/12Sev=Info/5IKE/0x6300000D  MODE_CFG_REPLY : Attribut = MODECFG_UNITY_PFS : , valeur = 0x00000000  58111:28:38.63908/24/12Sev=Info/5IKE/0x6300000E  MODE_CFG_REPLY : Attribut = APPLICATION_VERSION, valeur = version 8.4(4)1 de Cisco Systems, Inc ASA5505 établie par builders Thu 14-Jun-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 utilisant NAT-T  numéro de port, valeur = 0x00001194  58411:28:39.36708/24/12Sev=Debug/9IKE/0x63000093  La valeur pour le paramètre de temps imparti EnableDNSRedirection est 1  58511:28:39.36708/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-  &gt;TM:MsgID=84B4B653CurState :  TM_MODECFG_DONEEvent :  EV_MODECFG_DONE_SUC</p>	
--	---	--	--

<p>Construisez et envoyez DPD pour le client.</p>	<p>24 août 11:31:13 [IKEv1]IP = 64.102.156.87, type de keep-alive pour cette connexion : DPD  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, démarrant le temporisateur du rekey P1 : 82080 secondes.  24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, envoyant informant le message  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, construisant la charge utile vide d'informations parasites  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, construisant la charge utile d'informations parasites de qm  24 août 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE envoyant message (msgid=be8f7821) avec des charges utiles : HDR + les INFORMATIONS PARASITES (8) + ANNONCENT (11) + AUCUN (0)  longueurs totales : 92</p>	
	<p>=====&gt; de Dead Peer Detection de  ===== (DPD)</p>	
	<p>58811:28:39.79508/24/12Sev=Debug/7IKE/0x63000015  intf_data&amp;colon ; lcl=0x0501A8C0, mask=0x00FFFFFF, bcast=0xFF01A8C0, bcast_vra=0xFF07070A  58911:28:39.79508/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;SA:l_Cookie=D56197780D7BE3E5  R_Cookie=1B301D2DE710EDA0CurState :  CMN_MODECFG_PROGEvent : EV_INIT_P2  59011:28:39.79508/24/12Sev=Info/4IKE/0x63000056  A reçu une demande principale du gestionnaire : Gens du pays IP = 192.168.1.100, gw IP = 64.102.156.88, distant IP = 0.0.0.0  59111:28:39.79508/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;SA:l_Cookie=D56197780D7BE3E5  R_Cookie=1B301D2DE710EDA0CurState :  CMN_ACTIVEEvent : EV_NO_EVENT  59211:28:39.79508/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;QM:MsgID=0E83792ECurState :  QM_INITIALEvent : EV_INITIATOR  59311:28:39.79508/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;QM:MsgID=0E83792ECurState :  QM_BLD_MSG1Event : EV_CHK_PFS  59411:28:39.79608/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;QM:MsgID=0E83792ECurState :  QM_BLD_MSG1Event : EV_BLD_MSG  59511:28:39.79608/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;QM:MsgID=0E83792ECurState :  QM_SND_MSG1Event : EV_START_RETRY_TMR</p>	<p>QM initié, élaboration QM1 de la phase 2. Ce processus inclut :</p> <ul style="list-style-type: none"> <li>- Informations parasites</li> <li>- SA avec toutes les propositions de Phase 2 prises en charge par le client, le type de tunnel et le cryptage</li> <li>- Nonce</li> <li>- ID de client</li> <li>- Id de proxy</li> </ul>
	<p>59611:28:39.79608/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;QM:MsgID=0E83792ECurState :  QM_SND_MSG1Event : EV_SND_MSG  59711:28:39.79608/24/12Sev=Info/4IKE/0x63000013  ENVOYANT LE CHÊNE QM d'ISAKMP de &gt;&gt;&gt; *</p>	<p>Envoyez QM1.</p>

	(INFORMATIONS PARASITES, SA, NON, ID, ID) à 64.102.156.88	
	===== rapide du message 1 de mode de <===== (QM1)	
Recevez QM1.	24 août 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE A REÇU le message (msgid=e83792e) avec des charges utiles : HDR + INFORMATIONS PARASITES (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + AUCUN (0) longueurs totales : 1026	
Processus QM1. Configuration appropriée : 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 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, traitant la charge utile d'informations parasites 24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, traitant la charge utile SA 24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, traitant la charge utile de nonce 24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, charge utile d'IDENTIFICATEUR DE PROCESSUS 24 août 11:31:13 [IKEv1 DÉCODENT] le groupe = 'ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, ID ID_IPV4_ADDR reçu 192.168.1.100 24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, a reçu des données de système hôte distantes de proxy en charge utile d'ID : Adressez 192.168.1.100, Protocole 0, le port 0 24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, charge utile d'IDENTIFICATEUR DE PROCESSUS 24 août 11:31:13 [IKEv1 DÉCODENT] le groupe = 'ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, l'ID received--0.0.0.0--0.0.0.0 ID_IPV4_ADDR_SUBNET 24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, a reçu des données locales de sous-réseau de proxy IP en charge utile d'ID : Adressez 0.0.0.0, masque 0.0.0.0, Protocole 0, le port 0 24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, vieille SA QM IsRekeyed non trouvée par adr 24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, contrôle statique de crypto map, vérifiant la carte = la -MAP, = 10 seq... 24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, contrôle statique de crypto map sauté : Entrée de crypto map inachevée ! 24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, sélectionnant seulement des modes d'andUDP-Encapsuler-transport d'UDP-Encapsuler-tunnel définis par NAT-Traversal	

	<p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, sélectionnant seulement des modes d'andUDP-Encapsuler-transport d'UDP-Encapsuler-tunnel définis par NAT-Traversal</p> <p>24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, pair distant d'IKE configuré pour le crypto map : -dyne-MAP</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, traitant la charge utile d'IPSec SA</p>	
<p>Élaboration QM2. Configuration appropriée :</p> <pre> 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 </pre>	<p>24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, proposition d'IPSec SA # 12, transformant # 1 entrée globale d'IPSec SA d'acceptableMatches # 10</p> <p>24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, IKE : demande du SPI ! IPSEC : Nouveaux @ 0xcfdffc90 créés par SA embryonnaires, SCB : 0xCFDFFB58, direction : d'arrivée SPI : 0x9E18ACB2 ID de session : 0x00138000 VPIF numérique : 0x00000004 Type de tunnel : Ra Protocol : l'ESP Vie : 240 secondes</p> <p>24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, IKE ont obtenu le SPI de l'engine principale : SPI = 0x9e18acb2</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, oakley construisant le mode rapide</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, construisant la charge utile vide d'informations parasites</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, construisant la charge utile d'IPSec SA</p> <p>24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, IPSec du demandeur de ignorer réintroduisant la durée de 2147483 à 86400 secondes</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, construisant la charge utile de nonce d'IPSec</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, construisant l'ID de proxy</p> <p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, id de transmission de proxy :</p> <p>Serveur distant : 192.168.1.100Protocol 0Port 0</p>	

	Gens du pays subnet:0.0.0.0mask 0.0.0.0 Protocol 0Port 0 24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, envoyant la notification de VIE de RESPONDER au demandeur 24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, construisant la charge utile d'informations parasites de qm	
Envoyez QM2.	24 août 11:31:13 [IKEv1 DÉCODENT] le groupe = l'ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, responder d'IKE envoyant le 2ème paquet QM : id de msg = 0e83792e 24 août 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE envoyant message (msgid=e83792e) avec des charges utiles : HDR + les INFORMATIONS PARASITES (8) + SA (1) + le NONCE (10) + l'ID (5) + l'ID (5) + ANNONCENT (11) + AUCUN (0) longueurs totales : 184	
	=====> rapide du message 2 de mode de ===== (QM2)	
	60811:28:39.96208/24/12Sev=Info/4IKE/0x63000014 RECEVANT LE CHÊNE QM D'ISAKMP DE <<< * (INFORMATIONS PARASITES, SA, NON, ID, ID, ANNONCEZ : STATUS_RESP_LIFETIME) de 64.102.156.88	Recevez QM2.
	60911:28:39.96408/24/12Sev=Decode/11IKE/0x63000001 En-tête d'ISAKMP Demandeur COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Prochaine charge utile : Informations parasites Version (Hex):10 Type d'échange : Mode rapide Indicateurs : (Cryptage) MessageID(Hex):E83792E Length:188 Informations parasites de charge utile Prochaine charge utile : Association de sécurité Réservé : 00 Longueur de charge utile : 24 Données (dans l'hexa) : CABF38A62C9B88D1691E81F3857D6189534B2EC0 Association de sécurité de charge utile Prochaine charge utile : Nonce Réservé : 00 Longueur de charge utile : 52 DOI : IPsec Situation : (SIT_IDENTITY_ONLY)  Proposition de charge utile Prochaine charge utile : Aucun Réservé : 00 Longueur de charge utile : 40 Proposition # : 1 Protocol-id : PROTO_IPSEC_ESP	Processus QM2. Propositions choisies par expositions déchiffrées de charge utile.

	<p>Taille SPI : 4  # de transforme : 1  SPI : 9E18ACB2</p> <p>La charge utile transforment  Prochaine charge utile : Aucun  Réservé : 00  Longueur de charge utile : 28  Transformez # : 1  Transformer-id : ESP_3DES  Reserved2 : 0000  Type de vie : Secondes  Durée de vie (hexa) : 0020C49B  Mode d'encapsulation : Tunnel d'UDP  Algorithme d'authentification : SHA1  Nonce de charge utile  Prochaine charge utile : Identification  Réservé : 00  Longueur de charge utile : 24  Données (dans l'hexa) :  3A079B75DA512473706F235EA3FCA61F1D15D4CD  Identification de charge utile  Prochaine charge utile : Identification  Réservé : 00  Longueur de charge utile : 12  Type d'ID : ipv4 adres  ID de Protocol (UDP/TCP, etc...) : 0  Port : 0  ID Data&amp;colon ; 192.168.1.100  Identification de charge utile  Prochaine charge utile : Notification  Réservé : 00  Longueur de charge utile : 16  Type d'ID : Sous-réseau d'ipv4  ID de Protocol (UDP/TCP, etc...) : 0  Port : 0  ID Data&amp;colon ; 0.0.0.0/0.0.0.0  Notification de charge utile  Prochaine charge utile : Aucun  Réservé : 00  Longueur de charge utile : 28  DOI : IPsec  PROTOCOL-ID : PROTO_IPSEC_ESP  Taille de Spi : 4  Informez le type : STATUS_RESP_LIFETIME  SPI : 9E18ACB2  Data&amp;colon ;  Type de vie : Secondes  Durée de vie (hexa) : 00015180</p>	
	<p>61011:28:39.96508/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;QM:MsgID=0E83792ECurState :  QM_WAIT_MSG2Event : EV_RCVD_MSG  61111:28:39.96508/24/12Sev=Info/5IKE/0x63000045</p>	<p>Processus QM2.</p>

	<p>RESPONDER-LIFETIME annoncent ont la valeur de 86400 secondes  61211:28:39.96508/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;QM:MsgID=0E83792ECurState :  QM_WAIT_MSG2Event : EV_CHK_PFS  61311:28:39.96508/24/12Sev=Debug/7IKE/0x63000076</p>	
	<p>NAV Trace-&gt;QM:MsgID=0E83792ECurState :  QM_BLD_MSG3Event : EV_BLD_MSG  61411:28:39.96508/24/12Sev=Debug/7IKE/0x63000076  En-tête d'ISAKMP  Demandeur COOKIE:D56197780D7BE3E5  Responder COOKIE:1B301D2DE710EDA0  Prochaine charge utile : Informations parasites  Version (Hex):10  Type d'échange : Mode rapide  Indicateurs : (Cryptage)  MessageID(Hex):E83792E  Length:52</p> <p>Informations parasites de charge utile  Prochaine charge utile : Aucun  Réservé : 00  Longueur de charge utile : 24  Données (dans l'hexa) :  CDDC20D91EB4B568C826D6A5770A5CF020141236</p>	<p>Élaboration QM3. Charge utile déchiffrée pour QM3 affiché ici. Ces informations parasites de processus de ncludes.</p>
	<p>61511:28:39.96508/24/12Sev=Debug/7IKE/0x63000076  NAV Trace-&gt;QM:MsgID=0E83792ECurState :  QM_SND_MSG3Event : EV_SND_MSG  61611:28:39.96508/24/12Sev=Info/4IKE/0x63000013  ENVOYANT LE CHÊNE QM d'ISAKMP de &gt;&gt;&gt; *  (INFORMATIONS PARASITES) à 64.102.156.88</p>	<p>Envoyez QM3. Le client est maintenant prêt à chiffrer et déchiffrer.</p>
	<p>===== rapide du message 3 de mode de  &lt;===== (QM3)</p>	
<p>Recevez QM3.</p>	<p>24 août 11:31:13 [IKEv1]IP = 64.102.156.87,  IKE_DECODE A REÇU le message (msgid=e83792e)  avec des charges utiles : HDR + INFORMATIONS  PARASITES (8) + AUCUN (0) longueurs totales : 52</p>	
<p>Processus QM3.  Créez les index d'arrivée et sortants de paramètre de Sécurité (SPI).  Ajoutez l'artère statique pour l'hôte.  Configuration appropriée :</p> <pre>crypto ipsec transform- set TRA esp-aes esp- sha-hmac crypto ipsec security- association lifetime seconds 28800</pre>	<p>24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, traitant la charge utile d'informations parasites  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, chargeant tout l'IPSEC SAS  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, générant la clé rapide de mode !  24 août le groupe = l'ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, le NP chiffrent la consultation de règle pour l'inconnu assorti d'ACL de la -dyne-MAP 10 de crypto map : retourné cs_id=cc107410 ; rule=00000000  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, générant la</p>	



```
crypto ipsec
security-
association lifetime
kilobytes 4608000
crypto dynamic-map
DYN 10 set transform-
set TRA
crypto dynamic-map
DYN 10 set reverse-
route
```

clé rapide de mode !  
IPSEC : Nouveaux @ 0xccc9ed60 créés par SA  
embryonnaires,  
SCB : 0xCF7F59E0,  
Direction : sortant  
SPI : 0xC055290A  
ID de session : 0x00138000  
VPIF numérique : 0x00000004  
Type de tunnel : Ra  
Protocole : l'ESP  
Vie : 240 secondes  
IPSEC : Mise à jour terminée de l'hôte OBSA, SPI  
0xC055290A  
IPSEC : Création du contexte sortant VPN, SPI  
0xC055290A  
Indicateurs : 0x00000025  
SA : 0xccc9ed60  
SPI : 0xC055290A  
MTU : 1500 bytes  
VCID : 0x00000000  
Pair : 0x00000000  
SCB : 0xA5922B6B  
La Manche : 0xc82afb60  
IPSEC : Contexte sortant terminé VPN, SPI 0xC055290A  
Traitement VPN : 0x0015909c  
IPSEC : Nouveau sortant chiffrent la règle, SPI  
0xC055290A  
Adr de Src : 0.0.0.0  
Masque de Src : 0.0.0.0  
Adr de Dst : 192.168.1.100  
Masque de Dst : 255.255.255.255  
Ports de Src  
Stimulant : 0  
Inférieur : 0  
Op : ignorez  
Ports de Dst  
Stimulant : 0  
Inférieur : 0  
Op : ignorez  
Protocole : 0  
Protocole d'utilisation : faux  
SPI : 0x00000000  
Utilisation SPI : faux  
IPSEC : Sortant terminé chiffrent la règle, SPI  
0xC055290A  
ID de règle : 0xcb47a710  
IPSEC : Nouvelle règle sortante d'autorisation, SPI  
0xC055290A  
Adr de Src : 64.102.156.88  
Masque de Src : 255.255.255.255  
Adr de Dst : 64.102.156.87  
Masque de Dst : 255.255.255.255  
Ports de Src

Stimulant : 4500  
Inférieur : 4500  
Op : égal  
Ports de Dst  
Stimulant : 58506  
Inférieur : 58506  
Op : égal  
Protocole : 17  
Protocole d'utilisation : vrai  
SPI : 0x00000000  
Utilisation SPI : faux  
IPSEC : Règle sortante terminée d'autorisation, SPI  
0xC055290A  
ID de règle : 0xcdf3cfa0  
24 août le groupe = l'ipsec du DEBUG [IKEv1 de  
11:31:13], nom d'utilisateur = user1, IP = 64.102.156.87, le  
NP chiffrent la consultation de règle pour l'inconnu assorti  
d'ACL de la -dyne-MAP 10 de crypto map : retourné  
cs\_id=cc107410 ; rule=00000000  
24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur =  
user1, IP = 64.102.156.87, négociation de sécurité  
complète pour l'utilisateur (user1)Responder, SPI en  
entrée = 0x9e18acb2, sortant  
SPI = 0xc055290a  
24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13],  
nom d'utilisateur = user1, IP = 64.102.156.87, IKE  
a obtenu un msg KEY\_ADD pour SA : SPI = 0xc055290a  
IPSEC : Mise à jour terminée de l'hôte IBSA, SPI  
0x9E18ACB2  
IPSEC : Création du contexte d'arrivée VPN, SPI  
0x9E18ACB2  
Indicateurs : 0x00000026  
SA : 0xcdfffc90  
SPI : 0x9E18ACB2  
MTU : octets 0  
VCID : 0x00000000  
Pair : 0x0015909C  
SCB : 0xA5672481  
La Manche : 0xc82afb60  
IPSEC : Contexte d'arrivée terminé VPN, SPI  
0x9E18ACB2  
Traitement VPN : 0x0016219c  
IPSEC : Mise à jour du contexte sortant 0x0015909C  
VPN, SPI 0xC055290A  
Indicateurs : 0x00000025  
SA : 0xcc9ed60  
SPI : 0xC055290A  
MTU : 1500 bytes  
VCID : 0x00000000  
Pair : 0x0016219C  
SCB : 0xA5922B6B  
La Manche : 0xc82afb60  
IPSEC : Contexte sortant terminé VPN, SPI 0xC055290A

Traitement VPN : 0x0015909c  
IPSEC : Règle intérieure sortante terminée, SPI  
0xC055290A  
ID de règle : 0xcb47a710  
IPSEC : Règle externe sortante terminée SPD, SPI  
0xC055290A  
ID de règle : 0xcd3cfa0  
IPSEC : Nouvelle règle d'arrivée d'écoulement de tunnel,  
SPI 0x9E18ACB2  
Adr de Src : 192.168.1.100  
Masque de Src : 255.255.255.255  
Adr de Dst : 0.0.0.0  
Masque de Dst : 0.0.0.0  
Ports de Src  
Stimulant : 0  
Inférieur : 0  
Op : ignorez  
Ports de Dst  
Stimulant : 0  
Inférieur : 0  
Op : ignorez  
Protocole : 0  
Protocole d'utilisation : faux  
SPI : 0x00000000  
Utilisation SPI : faux  
IPSEC : Règle d'arrivée terminée d'écoulement de tunnel,  
SPI 0x9E18ACB2  
ID de règle : 0xcd15270  
IPSEC : Nouvelle règle d'arrivée de déchiffrement, SPI  
0x9E18ACB2  
Adr de Src : 64.102.156.87  
Masque de Src : 255.255.255.255  
Adr de Dst : 64.102.156.88  
Masque de Dst : 255.255.255.255  
Ports de Src  
Stimulant : 58506  
Inférieur : 58506  
Op : égal  
Ports de Dst  
Stimulant : 4500  
Inférieur : 4500  
Op : égal  
Protocole : 17  
Protocole d'utilisation : vrai  
SPI : 0x00000000  
Utilisation SPI : faux  
IPSEC : Règle d'arrivée terminée de déchiffrement, SPI  
0x9E18ACB2  
ID de règle : 0xce03c2f8  
IPSEC : Nouvelle règle d'arrivée d'autorisation, SPI  
0x9E18ACB2  
Adr de Src : 64.102.156.87  
Masque de Src : 255.255.255.255

	<p> Adr de Dst : 64.102.156.88  Masque de Dst : 255.255.255.255  Ports de Src  Stimulant : 58506  Inférieur : 58506  Op : égal  Ports de Dst  Stimulant : 4500  Inférieur : 4500  Op : égal  Protocole : 17  Protocole d'utilisation : vrai  SPI : 0x00000000  Utilisation SPI : faux  IPSEC : Règle d'arrivée terminée d'autorisation, SPI  0x9E18ACB2  ID de règle : 0xcf6f58c0  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13],  nom d'utilisateur = user1, IP = 64.102.156.87, broc :  KEY_UPDATE reçu, spi 0x9e18acb2  24 août groupe = ipsec du DEBUG [IKEv1 de 11:31:13],  nom d'utilisateur = user1, IP = 64.102.156.87, démarrant  le temporisateur du rekey P2 : 82080 secondes.  24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur =  user1, IP = 64.102.156.87, ajoutant l'artère statique pour  l'adresse du client : 192.168.1.100 </p>	
Phase 2 complet. Les deux côtés sont chiffants et déchiffants maintenant.	24 août 11:31:13 [IKEv1]Group = ipsec, nom d'utilisateur = user1, IP = 64.102.156.87, PHASE 2 S'EST TERMINÉ (msgid=0e83792e)	
Pour des clients matériels, un plus de message est reçu où le client envoie des informations sur se. Si vous regardez soigneusement, vous devriez trouver l'adresse Internet du client, le logiciel qui est exécuté sur le client, et l'emplacement et le nom d'EzVPN du logiciel	24 août 11:31:13 [IKEv1] : L'IP = le 10.48.66.23, IKE_DECODE ONT REÇU le message (msgid=91facca9) avec des charges utiles : HDR + les INFORMATIONS PARASITES (8) + ANNONCENT (11) + AUCUN (0) longueurs totales : 184 24 août DEBUG [IKEv1 de 11:31:13] : Groupe = EZ, nom d'utilisateur = Cisco, IP = 10.48.66.23, traitant la charge utile d'informations parasites 24 août DEBUG [IKEv1 de 11:31:13] : Le groupe = les EZ, nom d'utilisateur = Cisco, IP = 10.48.66.23, traitant informent la charge utile 24 août 11:31:13 [IKEv1 DÉCODENT] : DESCRIPTEUR DÉSUE(T) - INDEX 1 24 août 11:31:13 [IKEv1 DÉCODENT] : 0000 : 00000000 7534000B 62736E73 2D383731 ....u4. .bsns-871 0010 : 2D332E75 32000943 6973636F 20383731 -3.u2. <b>Cisco 871</b> 0020 : 7535000B 46484B30 39343431 32513675 u5..FHK094412Q6u 0030 : 36000932 32383538 39353638	

	<pre> 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 DEBUG [IKEv1 de 11:31:13] : Groupe = EZ, nom d'utilisateur = Cisco, IP = 10.48.66.23, traitant des informations parasites PSK 24 août 11:31:13 [IKEv1] : Groupe = EZ, nom d'utilisateur = Cisco, IP = 192.168.1.100, taille contradictoire d'informations parasites PSK 24 août DEBUG [IKEv1 de 11:31:13] : Le groupe = l'EZ, nom d'utilisateur = Cisco, IP = 10.48.66.23, vérification d'informations parasites PSK ont manqué ! </pre>	
--	--	--

## Vérification de tunnel

### ISAKMP

La sortie de la commande **SH de det d'IS SA de cri** est :

```

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

```

### IPsec

Puisque le Protocole ICMP (Internet Control Message Protocol) est utilisé pour déclencher le tunnel, seulement un IPsec SA est. Protocol 1 est ICMP. Notez que les valeurs SPI diffèrent de celles négociées dans met au point. C'est, en fait, le même tunnel après le rekey de Phase 2.

La sortie de la **crypto** commande **SH d'ipsec SA** est :

```

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
```

## [Informations connexes](#)

- [Article de Wikipedia sur IPsec](#)
- [Dépannage IPsec : Présentation et utilisation des commandes de débogage](#)
- [Support et documentation techniques - Cisco Systems](#)