# Configurer L2TP sur IPsec entre le PC Windows 8 et ASA à l'aide d'une clé pré-partagée

## Contenu

Introduction Conditions préalables **Conditions requises Restrictions Components Used Conventions** Informations générales Configuration Diagramme du réseau Configuration complète du tunnel Configuration ASA à l'aide d'Adaptive Security Device Manager (ASDM) Configuration ASA à l'aide de CLI Configuration du client L2TP/IPsec de Windows 8 Configuration du tunnel fractionné Configuration sur ASA Configuration sur le client L2TP/IPsec Vérification Dépannage Informations connexes

## Introduction

Ce document décrit comment configurer le protocole L2TP (Layer 2 Tunneling Protocol) sur IPsec à l'aide d'une clé pré-partagée entre Cisco Adaptive Security Appliance (ASA) et le client natif Windows 8.

La sécurité IPsec (L2TP over Internet Protocol) permet de déployer et d'administrer une solution VPN (Virtual Private Network) L2TP parallèlement aux services VPN IPsec et de pare-feu dans une plate-forme unique.

## Conditions préalables

## **Conditions requises**

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connectivité IP de la machine cliente à l'ASA. Pour tester la connectivité, essayez d'envoyer une requête ping à l'adresse IP de l'ASA à partir du point d'extrémité client et vice versa
- Assurez-vous que les ports UDP 500 et 4500 et le protocole ESP (Encapsulating Security

Payload) ne sont bloqués nulle part sur le chemin de la connexion.

### Restrictions

- L2TP sur IPsec prend uniquement en charge IKEv1. IKEv2 n'est pas pris en charge.
- L2TP avec IPsec sur l'ASA permet au LNS d'interagir avec des clients VPN natifs intégrés dans des systèmes d'exploitation tels que Windows, MAC OS X, Android et Cisco IOS. Seul L2TP avec IPsec est pris en charge, le L2TP natif lui-même n'est pas pris en charge sur ASA.
- La durée de vie minimale de l'association de sécurité IPsec prise en charge par le client Windows est de 300 secondes. Si la durée de vie de l'ASA est inférieure à 300 secondes, le client Windows l'ignore et le remplace par une durée de vie de 300 secondes.
- L'ASA prend uniquement en charge les authentifications PPP (Point-to-Point Protocol) PAP (Password Authentication Protocol) et CHAP (Microsoft Challenge-Handshake Authentication Protocol), versions 1 et 2, sur la base de données locale. Les protocoles EAP (Extensible Authentication Protocol) et CHAP sont exécutés par des serveurs d'authentification par proxy. Par conséquent, si un utilisateur distant appartient à un groupe de tunnels configuré avec les commandes **authentication eap-proxy** ou **authentication chap** et que l'ASA est configuré pour utiliser la base de données locale, cet utilisateur ne peut pas se connecter.

Types d'authentification PPP pris en charge

Les connexions L2TP sur IPsec sur l'ASA prennent uniquement en charge les types d'authentification PPP indiqués dans le tableau

	Prise en charge	des serveurs AAA et types d'authentification PPP		
Type de serveur AAA		Types d'authentification PPP pris en charge		
LOCAL		PAP, MSCHAPv1, MSCHAPv2		
	RADIUS	PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-Proxy		
	TACACS+	PAP, CHAP, MSCHAPv1		
	LDAP	PAP		
	NT	PAP		
	Kerberos	PAP		
	SDI	SDI		
Caractéristic	ques du type d'au	thentification PPP		
Mot clé	Type d'authentification	Caractéristiques		
chap.	CHAP	En réponse à la demande de confirmation du serveur, le client retourne le [demande de confirmation plus mot de passe] chiffré avec un nor d'utilisateur en texte clair. Ce protocole est plus sécurisé que le protocole PAP, mais il ne chiffre pas les données.		
eap-proxy	EAP	Active EAP qui permet au dispositif de sécurité de proxy du processur d'authentification PPP vers un serveur d'authentification RADIUS externe.		
	Microsoft CHAP,	Semblable à CHAP mais plus sécurisé en ce que le serveur stocke e		
ms-chap-v1	version 1	compare uniquement les mots de passe chiffrés plutôt que les mots de		
ms-chap-v2	Microsoft CHAP,	passe en texte clair comme dans CHAP. Ce protocole génère égalemer		
	Version, 2	une clé pour le chiffrement des données par MPPE.		
рар	PAP	Passe le nom d'utilisateur et le mot de passe en texte clair pendar l'authentification et n'est pas sécurisé.		

**Components Used** 

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA de la gamme Cisco 5515 qui exécute le logiciel version 9.4(1)
- Client L2TP/IPSec (Windows 8)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

### **Produits connexes**

Cette configuration peut également être utilisée avec l'appliance de sécurité de la gamme Cisco ASA 5500 8.3(1) ou version ultérieure.

### Conventions

Référez-vous à <u>Conventions des conseils techniques Cisco</u> pour plus d'informations sur les conventions du document

## Informations générales

Le protocole L2TP (Layer 2 Tunneling Protocol) est un protocole de tunnellisation VPN qui permet aux clients distants d'utiliser le réseau IP public pour communiquer en toute sécurité avec les serveurs de réseau d'entreprise privés. L2TP utilise le protocole PPP sur UDP (port 1701) pour tunnel les données.

Le protocole L2TP est basé sur le modèle client/serveur. La fonction est divisée entre le serveur de réseau L2TP (LNS) et le concentrateur d'accès L2TP (LAC). Le LNS s'exécute généralement sur une passerelle réseau telle que l'ASA dans ce cas, tandis que le LAC peut être un serveur d'accès réseau à distance (NAS) ou un périphérique de point de terminaison avec un client L2TP intégré tel que Microsoft Windows, Apple iPhone ou Android.

## Configuration

Cette section présente les informations permettant de configurer les fonctionnalités décrites dans ce document.

**Note**: Utilisez l'outil <u>Command Lookup Tool</u> (clients enregistrésseulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

**Note**: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

## Diagramme du réseau



## Configuration complète du tunnel

### Configuration ASA à l'aide d'Adaptive Security Device Manager (ASDM)

Procédez comme suit :

Étape 1. Connectez-vous à ASDM et accédez à Wizards > VPN Wizards > Ipsec (IKEv1) Remote Access VPN Wizard.

🚡 Cisco ASDM 7.2 for ASA - 10.106.44.216					
File View Tools	ols Wizards Window Help				
Home 🖧 Cont	Startup Wizard				
Devrine Lint	VPN Wizards			Site-to-site VPN Wizard	
Device List	н	igh Availability and Scalability Wizard		AnyConnect VPN Wizard	
Here Add Delete	U	nified Communication Wizard		Clientless SSL VPN Wizard	
Find:	Packet Capture Wizard		IPsec (IKEv1) Remote Access VPN Wizard		
Image: March 10, 105, 130, 63					

Étape 2. Une fenêtre de configuration VPN d'accès à distance s'affiche. Dans la liste déroulante, sélectionnez l'interface sur laquelle le tunnel VPN doit être interrompu. Dans cet exemple, l'interface externe est connectée au WAN et termine ainsi les tunnels VPN sur cette interface. Conservez la case Activer les sessions IPSec entrantes pour contourner les listes d'accès d'interface. Les listes d'accès aux autorisations de groupe et d'autorisation par utilisateur s'appliquent toujours au trafic vérifié de sorte que la nouvelle liste d'accès n'ait pas besoin d'être configurée sur l'interface externe pour permettre aux clients d'accéder aux ressources internes. Cliquez sur Next (Suivant).



Étape 3. Comme le montre cette image, choisissez le type de client en tant que **client Microsoft Windows utilisant L2TP sur IPSec** et **MS-CHAP-V1** et **MS-CHAP-V2** comme protocole d'authentification PPP puisque PAP n'est pas sécurisé et d'autres types d'authentification ne sont pas pris en charge avec la base de données LOCAL comme serveur d'authentification et cliquez sur **Suivant**.

🔄 VPN Wizard	×
VPN Wizard	Remote Access Client (Step 2 of)
Branch	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
E Lee	VPN Client Type:
	O Cisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product
Home	Microsoft Windows client using L2TP over IPsec
Corporate Network	Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.
THE THE	PAP CHAP MS-CHAP-V1 MS-CHAP-V2 EAP-PROXY
	Specify if the client will send tunnel group name as - username@tunnelgroup.
E-HUI IIII	Client will send tunnel group name as username@tunnelgroup.
Think	If pre-shared authentication is used with this option then DefaultRAGroup's
TTT	pre-shared key and ppp authentication are also modified.
- R-	
CO AVA	
	<pre>&lt; Back Next &gt; Finish Cancel Help</pre>

Étape 4. Choisissez la méthode d'authentification en tant que **clé pré-partagée** et tapez la clé prépartagée qui doit également être identique du côté client, puis cliquez sur **Suivant**, comme illustré dans cette image.

📑 VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
VTI WIZAIU	Where Charles Autometrication Precision and Tunnel Group Name (Step 3 of)         The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote client.         Authentication Method <ul> <li>Pre-shared key</li> <li>Pre-shared Key:</li> <li>Clsc0@123</li> <li>Certificate</li> <li>Certificate Signing Algorithm: rsa-sig</li> <li>Certificate Name:</li> <li>Challenge/response authentication (CRACK)</li> </ul> <ul> <li>Tunnel Group</li> </ul> For VPN clients using L2TP over IPsec with pre-shared key authentication, DefaultRAGroup tunnel group name to used.              Tunnel Group Name:         DefaultRAGroup
	< Back Next > Finish Cancel Help

Étape 5. Spécifiez une méthode pour authentifier les utilisateurs qui tentent des connexions L2TP sur IPsec. Vous pouvez utiliser un serveur d'authentification AAA externe ou sa propre base de données locale. Choisissez **Authentifier à l'aide de la base de données utilisateur locale** si vous voulez authentifier les clients par rapport à la base de données locale d'ASA et cliquez sur **Suivant.** 

**Note**: Reportez-vous à <u>Configurer l'authentification RADIUS pour les utilisateurs VPN</u> pour authentifier les utilisateurs à l'aide d'un serveur AAA externe.

C VPN Wizard	×
VPN Wizard	Client Authentication (Step 4 of)
Branch Branch Branch Branch Homo Corporate Network	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.
	< Back Next > Finish Cancel Help

Étape 6. Pour ajouter de nouveaux utilisateurs à la base de données locale pour l'authentification des utilisateurs, entrez le nom d'utilisateur et le mot de passe, puis cliquez sur **AJOUTER** ou d'autres comptes d'utilisateurs existants dans la base de données peuvent être utilisés, comme illustré dans cette image. Cliquez sur **Next (Suivant).** 

🔁 VPN Wizard			×
VPN Wizard Branch	User Accounts (Step 5 of 11) Add new users into the user authention or to remove them from the database Users/AAA > User Accounts in the mat	ication database. To edit existin e, go to Configuration > Device ain ASDM window.	g entries in the database Management >
Corporate Network	User to Be Added Username: test Password (optional): •••• Confirm Password (optional): ••••	Add >> Delete	
		< Back Next > Fi	nish Cancel Help

Étape 7. Dans la liste déroulante, sélectionnez le pool d'adresses à utiliser pour attribuer une adresse IP aux clients. Pour créer un nouveau pool d'adresses, cliquez sur **Nouveau**, comme illustré dans cette image.

C VPN Wizard		x
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Franch Franch Franch Franch Franch Franch Franch	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN dients.	N
Corporate Network	Tunnel Group Name : DefaultRAGroup	_
THE THE	Pool Name:  New	
	Pool Settings	
244UM	Range Start Address:	
T	Range End Address:	
	Subnet Mask:	
	< Back Next > Finish Cancel He	elp

Étape 8. La boîte de dialogue Ajouter un pool IPv4 apparaît.

- 1. Saisissez le nom du nouveau pool d'adresses IP.
- 2. Entrez les adresses IP de début et de fin.
- 3. Entrez le masque de sous-réseau et cliquez sur OK.

is VPN Wizard			23
VPN Wizard	Address Pool (Step	6 of 11)	
Branch Franch Soft	Enter a pool of loo dients.	cal addresses to be used for assigning dynamic IP addresses to remote VPN	
Home	📑 Add IPv4 Pool		
Corporate Network	Name:	Address-pool	
Ection 10	Starting IP Address:	192.168.1.1	
	Ending IP Address:	192.168.1.254	
LUU III	Subnet Mask:	255.255.255.0	
The	ОК	Cancel Help	
		Subheil Plask.	
		< Back Next > Finish Cancel Hel	p

Étape 9. Vérifiez les paramètres du pool et cliquez sur Suivant.

VPN Wizard	
VPN Wizard	Address Pool (Step 6 of 11)
Branch	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.
Corporate Network	Tunnel Group Name : DefaultRAGroup
THE THE	Pool Name: Address-pool   New
	Pool Settings
- UIIIII	Range Start Address: 192.168.1.1
T	Range End Address: 192.168.1.254
- 1-4L	Subnet Mask: 255.255.0
C D	
	< Back Next > Finish Cancel Help

Étape 10. Configurez les attributs à transmettre aux clients ou laissez-les vides et cliquez sur **Suivant.** 

T VPN Wizard		×
VPN Wizard	Attributes Pushed to Client (Optional) (S	5tep 7 of 11)
Branch	Attributes you configure below are pushed ASA. If you do not want an attribute push	d to the VPN client when the client connects to the ned to the client, leave the corresponding field blank.
Corporate Notwork	Tunnel Group:	DefaultRAGroup
C.I.Ma	Primary DNS Server:	8.8.8.8
	Secondary DNS Server:	4.4.4.2
TATA	Primary WINS Server:	
	Secondary WINS Server:	
	Default Domain Name:	cisco.com
		< Back Next > Finish Cancel Help

Étape 11 : Assurez-vous que la case Activer le secret de transfert parfait (PFS) n'est pas cochée car certaines plates-formes clientes ne prennent pas en charge cette fonctionnalité. Activez la transmission tunnel partagée pour permettre aux utilisateurs distants d'avoir un accès crypté simultané aux ressources définies ci-dessus, et l'accès non crypté à la case Internet est décoché, ce qui signifie que la transmission tunnel complète est activée dans laquelle tout le trafic (y compris le trafic Internet) de la machine cliente sera envoyé à l'ASA via le tunnel VPN. Cliquez sur Next (Suivant).

Te VPN Wizard	
VPN Wizard	IPsec Settings (Optional) (Step 8 of 11)
Branch Branch Fisp Home	Network Address Translation (NAT) is used to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN. To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the Exempt Networks field blank.
Corporate Network	Interface:
	Exempt Networks:
	Enable Perfect Forwarding Secrecy (PFS)
	Diffie-Hellman Group:
	< <u>Back</u> <u>Next</u> > <u>Finish</u> <u>Cancel</u> <u>H</u> elp

Étape 12. Examinez les informations récapitulatives, puis cliquez sur Terminer.



### Configuration ASA à l'aide de CLI

Étape 1. Configurez les paramètres de la stratégie IKE Phase 1.

Cette politique est utilisée pour protéger le trafic de contrôle entre homologues (c'est-à-dire, elle protège la clé pré-partagée et les négociations de phase 2).

```
ciscoasa(config)#crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#hash sha
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#lifetime 86400
ciscoasa(config-ikev1-policy)#exit
Étape 2. Configurez Transform-set.
```

Il contient les paramètres de stratégie IKE de phase 2 qui sont utilisés pour protéger le trafic de données. Puisque le client L2TP/IPsec Windows utilise le mode de transport IPsec, définissez le mode sur transport. La valeur par défaut est le mode tunnel.

ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport **Étape 3. Configurez la carte dynamique.** 

Lorsque les clients Windows obtiennent une adresse IP dynamique pour le FAI ou le serveur

DHCP local (par exemple, un modem), ASA ne connaît pas l'adresse IP de l'homologue et cela pose un problème dans la configuration d'un homologue statique sur l'extrémité ASA. La configuration de chiffrement dynamique doit donc être abordée dans laquelle tous les paramètres ne sont pas nécessairement définis et les paramètres manquants sont appris dynamiquement ultérieurement, à la suite de la négociation IPSec du client.

ciscoasa(config)#crypto dynamic-map outside\_dyn\_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA Étape 4. Lier la carte dynamique à la carte de chiffrement statique et appliquer la carte de chiffrement et activer IKEv1 sur l'interface externe

La carte de chiffrement dynamique ne peut pas être appliquée sur une interface et donc la lier à la carte de chiffrement statique. Les jeux de chiffrement dynamiques doivent être les cartes de chiffrement de priorité la plus basse dans le jeu de cartes de chiffrement (c'est-à-dire qu'ils doivent avoir les numéros de séquence les plus élevés) afin que l'ASA évalue d'autres cartes de chiffrement en premier. Il examine le jeu de cartes de chiffrement dynamique uniquement lorsque les autres entrées de cartes (statiques) ne correspondent pas.

ciscoasa(config)#crypto map outside\_map 65535 ipsec-isakmp dynamic outside\_dyn\_map ciscoasa(config)#crypto map outside\_map interface outside ciscoasa(config)#crypto ikev1 enable outside Étape 5. Créer un pool d'adresses IP

Créez un pool d'adresses à partir duquel les adresses IP sont attribuées dynamiquement aux clients VPN distants. Ignorez cette étape pour utiliser le pool existant sur ASA.

ciscoasa(config)#ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0 Étape 6. Configurer la stratégie de groupe

Identifiez la stratégie de groupe comme interne, ce qui signifie que les attributs sont extraits de la base de données locale.

ciscoasa(config)#group-policy L2TP-VPN internal

**Note**: Les connexions L2TP/IPsec peuvent être configurées avec une stratégie de groupe par défaut (DfltGrpPolicy) ou une stratégie de groupe définie par l'utilisateur. Dans les deux cas, la stratégie de groupe doit être configurée pour utiliser le protocole de tunnellisation L2TP/IPsec. configurez l2tp-ipsec sur l'attribut de protocole VPN sur la stratégie de groupe par défaut qui sera héritée de la stratégie de groupe définie par l'utilisateur si l'attribut vpn-protocol n'est pas configuré dessus.

Configurez les attributs tels que le protocole de tunnel vpn (dans notre cas, il s'agit de l2tp-ipsec), le nom de domaine, l'adresse IP du serveur DNS et WINS et les nouveaux comptes d'utilisateurs

ciscoasa(config)#group-policy L2TP-VPN attributes

ciscoasa(config-group-policy)#dns-server value 8.8.8.8 4.4.4.2

ciscoasa(config-group-policy)#vpn-tunnel-protocol l2tp-ipsec

ciscoasa(config-group-policy)#default-domain value cisco.com

Configurez les noms d'utilisateur et les mots de passe sur le périphérique en plus de l'utilisation de AAA. Si l'utilisateur est un client L2TP qui utilise Microsoft CHAP version 1 ou version 2 et que l'ASA est configuré pour s'authentifier sur la base de données locale, le mot clé mschap doit être inclus. Par exemple, username <username> password <password> mschap.

ciscoasa(config-group-policy)# username test password test mschap Étape 7. Configurer le groupe de tunnels

Créez un groupe de tunnels avec la commande **tunnel-group**, et spécifiez le nom du pool d'adresses locales utilisé pour allouer l'adresse IP au client. Si la méthode d'authentification est une clé pré-partagée, le nom du groupe de tunnels doit être DefaultRAGroup car il n'y a aucune option sur le client pour spécifier le groupe de tunnels et il s'arrête donc sur le groupe de tunnels par défaut uniquement. Lier la stratégie de groupe à tunnel-group à l'aide de la commande default-group-policy

```
ciscoasa(config)#tunnel-group DefaultRAGroup general-attributes
ciscoasa(config-tunnel-general)#address-pool Address-pool
ciscoasa(config-tunnel-general)#default-group-policy L2TP-VPN
ciscoasa(config-tunnel-general)#exit
```

**Note**: Le profil de connexion par défaut (groupe de tunnels), DefaultRAGroup, doit être configuré, si l'authentification basée sur une clé pré-partagée est effectuée. Si l'authentification basée sur un certificat est effectuée, un profil de connexion défini par l'utilisateur peut être choisi en fonction des identificateurs de certificat

Utilisez la commande **tunnel-group ipsec-attribute** pour passer en mode de configuration ipsecattribute afin de définir la clé pré-partagée.

ciscoasa(config)# tunnel-group DefaultRAGroup ipsec-attributes ciscoasa(config-tunnel-ipsec)# ikev1 pre-shared-key C!sc0@123 ciscoasa(config-tunnel-ipsec)#exit

Configurez le protocole d'authentification PPP avec la commande **authentication type** à partir du mode tunnel group ppp-attribute. Désactivez CHAP qui est activé par défaut car il n'est pas pris en charge si le serveur AAA est configuré en tant que base de données locale.

ciscoasa(config)#tunnel-group DefaultRAGroup ppp-attributes ciscoasa(config-ppp)#no authentication chap ciscoasa(config-ppp)#authentication ms-chap-v2 ciscoasa(config-ppp)#exit Étape 8. Configurer l'exemption NAT

Configurez NAT-Exemption de sorte que les clients puissent accéder aux ressources internes connectées aux interfaces internes (dans cet exemple, les ressources internes sont connectées à l'interface interne).

ciscoasa(config)#object network L2TP-Pool ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0 ciscoasa(config-network-object)#exit ciscoasa(config)# nat (inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp route-lookup Exemple complet de configuration

crypto ikev1 policy 10 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 exit crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport crypto dynamic-map outside\_dyn\_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA crypto map outside\_map 65535 ipsec-isakmp dynamic outside\_dyn\_map crypto map outside\_map interface outside crypto ikev1 enable outside ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0 group-policy L2TP-VPN internal group-policy L2TP-VPN attributes vpn-tunnel-protocol l2tp-ipsec default-domain value cisco.com username test password test mschap exit tunnel-group DefaultRAGroup general-attributes address-pool Address-pool default-group-policy L2TP-VPN exit tunnel-group DefaultRAGroup ipsec-attributes ikev1 pre-shared-key C!sc0@123 exit tunnel-group DefaultRAGroup ppp-attributes no authentication chap authentication ms-chap-v2 exit object network L2TP-Pool subnet 192.168.1.0 255.255.255.0 exit nat(inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp

#### Configuration du client L2TP/IPsec de Windows 8

route-lookup

1. Ouvrez le Panneau de configuration et sélectionnez Centre Réseau et partage.



2. Choisissez Configurer une nouvelle connexion ou une nouvelle option réseau.

¥	Network and Sharing Center	- 🗆 🗙	
🛞 🌛 👻 🕈 騹 « All Control P	anel Items	✓ ♂ Search Control Panel	
Control Panel Home	View your basic network information and set up connections		
Change adapter settings	View your active networks		
Change advanced sharing settings	Network 2 Public network	Access type: No Internet access Connections: Ethernet	
	hange vour networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN connection; or set up a router or access point. Troubleshoot problems Diagnose and repair network problems, or get troubleshooting information.		
See also			
HomeGroup			
Windows Firewall			

3. Sélectionnez Se connecter à un lieu de travail, puis cliquez sur Suivant.

🗆 X

\_

4. Cliquez sur Utiliser ma connexion Internet (VPN).



5. Entrez l'adresse IP de l'interface WAN ou du nom de domaine complet d'ASA et tout nom de l'adaptateur VPN qui est significatif localement, puis cliquez sur **Créer**.

			-		~
€	Connect to a Workpl	ace			
	Type the Internet addre	ess to connect to			
	Your network administrator c				
	Internet address:	172.16.1.2			
	Destination name:	L2TP VPN			
	Use a smart card				
	Remember my credentials				
	Allow other people to This antice allows and	use this connection			
	This option allows any	yone with access to this computer to use this connection.			
		Crea	te	Cano	cel

6. Dans Centre Réseau et partage, sélectionnez **Modifier les paramètres de la carte** dans le volet gauche de la fenêtre.



7. Cliquez avec le bouton droit sur l'adaptateur récemment créé pour VPN L2TP et sélectionnez **Propriétés.** 



8. Accédez à l'onglet **Sécurité**, choisissez le type de VPN en tant que **protocole de tunnellisation de couche 2 avec IPsec (L2TP/IPsec)**, puis cliquez sur **Paramètres avancés**.

L2TP VPN Properties							
General Options Security Networking Sharing							
Type of VPN:							
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)							
Data encryption:							
Require encryption (disconnect if server declines)							
Authentication							
O Use Extensible Authentication Protocol (EAP)							
v							
Proportion							
Fropenies							
<ul> <li>Allow these protocols</li> </ul>							
Upprogrammed password (PAP)							
Challenge Handshake Authentication Protocol (CHAP)							
Mismaat CHAR Version 2 (MS CHAR v2)							
password (and domain, if any)							
OK Cancel							

9. Entrez la clé pré-partagée mentionnée dans le groupe de tunnels **DefaultRAGroup** et cliquez sur **OK**. Dans cet exemple, C!sc0@123 est utilisé comme clé pré-partagée.

Advanced Properties					
L2TP					
Use preshared key for authentication					
Key: C!sc0@123					
✓ Use certificate for authentication ✓ Verify the Name and Usage attributes of the server's certificate					
OK Cancel					

10. Sélectionnez la méthode d'authentification Allow these protocols (Autoriser ces protocoles) et assurez-vous que seule la case à cocher "**Microsoft CHAP Version 2 (MS-CHAP v2)** est cochée et cliquez sur **OK**.

General Options Security Networking Sharing						
Type of VPN:						
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)						
Advanced settings						
Require encryption (disconnect if server declines)						
Authentication O Use Extensible Authentication Protocol (EAP)						
Properties						
<ul> <li>Allow these protocols</li> <li>Unencrypted password (PAP)</li> <li>Challenge Handshake Authentication Protocol (CHAP)</li> <li>Microsoft CHAP Version 2 (MS-CHAP v2)</li> <li>Automatically use my Windows logon name and</li> </ul>						
OK Cancel						

11. Sous Connexions réseau, cliquez avec le bouton droit sur l'adaptateur VPN L2TP et choisissez **Connect/Disconnect**.



12. L'icône Réseaux s'affiche et cliquez sur Connect sur la connexion VPN L2TP.

<b>Q</b>	Network Connections	Networks	
	ternet > Network Connections > C	Connections	
Organize  Start this connection  Fthernet	Rename this connection Delete this connection >>	Network 2	Limited 97
Network 2 vmxnet3 Ethernet Adapter	Disconnected WAN Miniport (L2TP)		
		LZTP VPN	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
			<u>C</u> onnect

13. Entrez les informations d'identification de l'utilisateur et cliquez sur OK.

Networks
Connecting to 172.16.1.2
Network Authentication
User name
Password
Domain:
OK Cancel

Si les paramètres requis sont mis en correspondance aux deux extrémités, la connexion L2TP/IPsec sera établie.



### Configuration du tunnel fractionné

La tunnellisation fractionnée est une fonction que vous pouvez utiliser pour définir le trafic des sous-réseaux ou des hôtes à chiffrer. Ceci implique la configuration d'une liste de contrôle d'accès (ACL) associée à cette fonctionnalité. Le trafic des sous-réseaux ou des hôtes qui est défini sur cette liste de contrôle d'accès est chiffré via le tunnel depuis l'extrémité client et les routes de ces sous-réseaux sont installées dans la table de routage du PC. ASA intercepte le message DHCPINFORM d'un client et répond avec le masque de sous-réseau, le nom de domaine et les routes statiques sans classe.

### Configuration sur ASA

ciscoasa(config)# access-list SPLIT standard permit 10.1.1.0 255.255.255.0
ciscoasa(config)# group-policy DefaultRAGroup attributes
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified
ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT
ciscoasa(config-group-policy)# intercept-dhcp 255.255.255 enable
Config-group-policy)# access
Config-group-policy Config-group-policy
Config-group-policy Config-group-policy
Config-group-policy Config-group-policy
Config-group-policy Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy
Config-group-policy

Configuration sur le client L2TP/IPsec

1. Cliquez avec le bouton droit sur l'adaptateur VPN L2TP et choisissez Propriétés.



2. Accédez à l'onglet Réseau, choisissez Protocole Internet version 4 (TCP/IPv4), puis cliquez sur **Propriétés.** 

L2TP VPN Properties	×					
General Options Security Networking Sharing						
This connection uses the following items:						
Internet Protocol Version 6 (TCP/IPv6)						
Internet Protocol Version 4 (TCP/IPV4)     Image: A second s	•					
Client for Microsoft Networks						
🚱 Install 💮 Uninstall Properties	1					
Description						
Transmission Control Protocol/Internet Protocol. The default						
wide area network protocol that provides communication across diverse interconnected networks.						
	- 1					
OK Cancel						

3. Cliquez sur l'option Avancé.

Internet Protocol Version 4 (To	CP/IPv4) Properties ? ×
General	
You can get IP settings assigned auto supports this capability. Otherwise, you administrator for the appropriate IP set	matically if your network u need to ask your network tings.
Obtain an IP address automatica	lly
Use the following IP address:	
IP address:	· · ·
Obtain DNS server address autor     O Use the following DNS server ad     Preferred DNS server:	matically dresses:
Alternate DNS server:	
	Advanced OK Cancel

4. Décochez la case Utiliser la passerelle par défaut sur l'option réseau distant et cliquez sur OK.

Advanced TCP/IP Settings ? ×
IP Settings DNS WINS
This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.
Use default gateway on remote network Disable class based route addition
Automatic metric Interface metric:
OK Cancel

## Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

**Note**: L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

• show crypto ikev1 sa - Affiche toutes les SA IKE actuelles sur un homologue.

```
ciscoasa# show crypto ikev1 sa
IKEv1 SAs:
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:

#### 10.1.1.2

Type : user Role : responder Rekey : no

#### State : MM\_ACTIVE

• show crypto ipsec sa - Affiche toutes les SA IPsec actuelles sur un homologue.

ciscoasa# show crypto ipsec sa interface: outside Crypto map tag:

#### outside\_dyn\_map

, seq num: 10, local addr: 172.16.1.2

local ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/

#### 17/1701

```
)
```

remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/

#### 17/1701

)

current\_peer: 10.1.1.2, username: test

dynamic allocated peer ip: 192.168.1.1

dynamic allocated peer ip(ipv6): 0.0.0.0

#### #pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29

#### #pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
#post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0

```
#TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 0
 local crypto endpt.: 172.16.1.2/0, remote crypto endpt.: 10.1.1.2/0
 path mtu 1500, ipsec overhead 58(36), media mtu 1500
 PMTU time remaining (sec): 0, DF policy: copy-df
 ICMP error validation: disabled, TFC packets: disabled
 current outbound spi: E8AF927A
 current inbound spi : 71F346AB
inbound esp sas:
 spi: 0x71F346AB (1911768747)
    transform: esp-3des esp-sha-hmac no compression
    in use settings ={RA, Transport, IKEv1, }
    slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
    sa timing: remaining key lifetime (kB/sec): (237303/3541)
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
     0x0000000 0x0000003
outbound esp sas:
 spi: 0xE8AF927A (3903820410)
    transform: esp-3des esp-sha-hmac no compression
    in use settings ={RA, Transport, IKEv1, }
    slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
    sa timing: remaining key lifetime (kB/sec): (237303/3541)
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
     0x0000000 0x0000001
```

• show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverlpSec - Affiche des informations détaillées sur les connexions L2TP sur IPsec.

ciscoasa# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec

Session Type: IKEv1 IPsec Detailed

Username : test

Index : 1

Assigned IP : 192.168.1.1

Public IP : 10.1.1.2

Protocol	: IKEv1 IPsec L2TPOverIPsec					
License : Other VPN						
Encryption	:	IKEv1: (1)3DE	IPsec:	(1)3DES	L2TPOverIPsec:	(1)none
Hashing	:	IKEv1: (1)SHA	1 IPsec:	(1) SHA1	L2TPOverIPsec:	(1)none
Bytes Tx	:	1574		Bytes Rx	: 12752	
Pkts Tx	:	29		Pkts Rx	: 118	
Pkts Tx Drop	:	0		Pkts Rx 1	Drop : O	

```
Group Policy : L2TP-VPN
```

Tunnel Group : DefaultRAGroup

Duration : 0h:04m:05s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0a6a2577000010005557d3a0 Security Grp : none IKEv1 Tunnels: 1 IPsec Tunnels: 1

#### IKEv1:

Tunnel ID : 1.1 UDP Src Port : 500 IKE Neg Mode : Main Encryption : 3DES Rekey Int (T): 28800 Seconds D/H Group : 2 Filter Name :

L2TPOverIPsec Tunnels: 1

UDP Dst Port : 500 Auth Mode : preSharedKeys Hashing : SHA1 Rekey Left(T): 28555 Seconds

#### IPsec:

Tunnel ID :	1.2			
Local Addr :	172.16.1.2/255.255.255	.255/17/1701		
Remote Addr :	10.1.1.2/255.255.255.255/17/1701			
Encryption :	3DES	Hashing :	SHA1	
Encapsulation:	Transport			
Rekey Int (T):	3600 Seconds	Rekey Left(T):	3576 Seconds	
Rekey Int (D):	250000 K-Bytes	Rekey Left(D):	250000 K-Bytes	
Idle Time Out:	30 Minutes	Idle TO Left :	29 Minutes	
Bytes Tx :	1574	Bytes Rx :	12752	
Pkts Tx :	29	Pkts Rx :	118	

#### L2TPOverIPsec:

Tunnel ID : 1.3

Username : test

#### Assigned IP : 192.168.1.1

#### Public IP : 10.1.1.2

Idle Time Out	::	30 Minutes	Idle TO Left	:	27 Minutes
Client OS	:	Microsoft			
Client OS Ver	::	6.2			
Bytes Tx	:	475	Bytes Rx	:	9093
Pkts Tx	:	18	Pkts Rx	:	105

Sur ASDM, sous **Monitoring > VPN > VPN Statistics > Sessions**, les informations générales relatives à la session VPN sont visibles. Les sessions L2TP sur IPsec peuvent être filtrées par **IPsec (IKEv1) Remote Access > Protocol > L2TP sur IPsec**.

File View Tools Wizards Wind	low	Help										Type topic to search G	°	Ī
🔥 Home 🖓 Configuration [ Mo	onitor	ring 🔒 Save 🔇	Refresh 📀 Back 🜔	Forward 🢡 Help									cisco	
Device List 🗗 🕂 🗡		Monitoring > VPN > <sup>1</sup>	VPN Statistics > Session	<u>s</u>										
🗣 Add 📋 Delete 🚿 Connect	I F													
Find: Go		Туре		Active			Cumulative			Peak Concurrent	t	Inactive		
→■         10.105.130.63         ▲           →■         10.105.130.92         ●           ■         10.105.130.98         ■           ■         10.105.130.98         ■           ■         10.105.130.91         ■           ■         10.105.130.153         ■           ■         10.105.130.211         ■           ■         10.105.130.214         ■           ■         10.105.130.225         ▼		IKEv 1 IPsec/L2TP IPse	ec v1) Remote Access 💌] [Pr	otocol	[LZTP Over IPsec	1				15		1		
VPN Statistics     Sessions		Username	Group Policy Connection Profile	Assigned IP Address Public(Peer) IP Address	Protocol Encryption	Login Time Duration		Client(Peer) Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token			Details	
VPN Cluster Loads     Crypto Statistics     Compression Statistics     Ercryption Statistics     Global InE//Parc Statistics     WAC Season Sammar y     Protocol Statistics     V.A.1 Mapping Sessions     V.A.1 Mapping Sessions     V.A.1 Mapping Sessions     V.A.1 Mapping Sessions		test	DefaultAGroup DefaultRAGroup	192,168,1.1 64,103,236,179	JREVI IPSec (ZTPOverIPse JREVI: (1)3DES IPsec: (1	√05:45:13 UTC Sat May 9 2 (0h:03m:238	2015	Microsoft  6:1	1422 24688	Unknown			Ping	

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

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

Attention : Sur l'ASA, vous pouvez définir différents niveaux de débogage ; par défaut, le niveau 1 est utilisé. Si vous modifiez le niveau de débogage, la verbosité des débogages pourrait augmenter. Faites ceci avec prudence, surtout dans les environnements de production !

Utilisez les **commandes debug** suivantes **avec prudence** afin de résoudre les problèmes liés au tunnel VPN.

debug crypto ikev1 - affiche les informations de débogage sur IKE

• debug crypto ipsec - affiche les informations de débogage sur IPsec

Voici la sortie de débogage pour une connexion L2TP sur IPSec réussie :

```
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ SA (1) + VENDOR (13) + VENDOR (13)
```

```
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Oakley proposal is acceptable
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal RFC VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal ver 02 VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received Fragmentation VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing IKE SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2,
```

#### IKE SA Proposal # 1, Transform # 5 acceptable Matches global IKE entry # 2

May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ISAKMP SA payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Traversal VID ver RFC payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Fragmentation VID + extended capabilities payload May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE\_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 124 May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500 May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE\_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 260 May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ke payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ISA\_KE payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing nonce payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload May 18 04:17:18 [IKEv1 DEBUG] IP = 10.1.1.2, computing NAT Discovery hash May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ke payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing nonce payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Cisco Unity VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing xauth V6 VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send IOS VID May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 2000001) May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash May 18 04:17:18 [IKEv1]IP = 10.1.1.2,

#### Connection landed on tunnel\_group DefaultRAGroup

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating keys for Responder... May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE\_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304 May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500

```
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ ID (5) + HASH (8) + NONE (0) total length : 64
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received
10.1.1.2
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

## Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Connection landed on tunnel\_group DefaultRAGroup May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing ID payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE\_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 84 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

PHASE 1 COMPLETED

```
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alive type for this connection: None
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alives configured on but peer does not support keep-
alives (type = None)
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P1 rekey timer:
21600 seconds.
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1 DECODE]IP = 10.1.1.2, IKE Responder starting QM: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR
+ HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 300
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received
10.1.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

#### Received remote Proxy Host data in ID Payload: Address 10.1.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID\_IPV4\_ADDR ID received 172.16.1.2 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received local Proxy Host data in ID Payload: Address 172.16.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

#### L2TP/IPSec session detected.

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, QM IsRekeyed old sa not found by addr May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

#### Static Crypto Map check, map outside\_dyn\_map, seq = 10 is a successful match

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Remote Peer configured for crypto map: outside\_dyn\_map May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing IPSec SA payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, I

#### PSec SA Proposal # 2, Transform # 1 acceptable

Matches global IPSec SA entry # 10 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE: requesting SPI! IPSEC: New embryonic SA created @ 0x00007fffe13ab260, SCB: 0xE1C00540, Direction: inbound SPI : 0x7AD72E0D Session ID: 0x00001000 VPIF num : 0x0000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got SPI from key engine: SPI = 0x7ad72e0dMay 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, oakley constucting quick mode May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing blank hash payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec SA payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec nonce pavload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing proxy ID May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2,

#### Transmitting Proxy Id:

Remote host: 10.1.1.2 Protocol 17 Port 1701

#### Local host: 172.16.1.2 Protocol 17 Port 1701

```
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing qm hash payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Responder sending 2nd
QM pkt: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=1) with payloads : HDR +
HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR
+ HASH (8) + NONE (0) total length : 52
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, loading all IPSEC SAs
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
```

encrypt\_rule=00000000; tunnelFlow\_rule=00000000 May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key! IPSEC: New embryonic SA created @ 0x00007fffe1c75c00, SCB: 0xE13ABD20, Direction: outbound : 0x8C14FD70 SPT Session ID: 0x00001000 VPIF num : 0x0000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0x8C14FD70 IPSEC: Creating outbound VPN context, SPI 0x8C14FD70 Flags: 0x00000205 SA : 0x00007fffe1c75c00 SPI : 0x8C14FD70 MTU : 1500 bytes VCID : 0x0000000 Peer : 0x0000000 SCB : 0x0AC609F9 Channel: 0x00007fffed817200 IPSEC: Completed outbound VPN context, SPI 0x8C14FD70 VPN handle: 0x000000000028d4 IPSEC: New outbound encrypt rule, SPI 0x8C14FD70 Src addr: 172.16.1.2 Src mask: 255.255.255.255 Dst addr: 10.1.1.2 Dst mask: 255.255.255.255

Src ports

**Upper: 1701** 

Lower: 1701

Op : equal

Dst ports

**Upper: 1701** 

Lower: 1701

Op : equal

#### Protocol: 17

```
Use protocol: true
   SPI: 0x0000000
   Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c763d0
IPSEC: New outbound permit rule, SPI 0x8C14FD70
  Src addr: 172.16.1.2
   Src mask: 255.255.255.255
  Dst addr: 10.1.1.2
   Dst mask: 255.255.255.255
   Src ports
    Upper: 0
    Lower: 0
    Op : ignore
   Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x8C14FD70
   Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c76a00
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, Security negotiation complete for
User () Responder, Inbound SPI = 0x7ad72e0d, Outbound SPI = 0x8c14fd70
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got a KEY_ADD msg for
SA: SPI = 0x8c14fd70
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
  Direction: inbound
  SPI
       : 0x7AD72E0D
   Session ID: 0x00001000
  VPIF num : 0x0000002
  Tunnel type: ra
   Protocol : esp
   Lifetime
            : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x7AD72E0D
IPSEC: Creating inbound VPN context, SPI 0x7AD72E0D
   Flags: 0x0000206
   SA : 0x00007fffe13ab260
  SPI : 0x7AD72E0D
  MTU : 0 bytes
   VCID : 0x0000000
   Peer : 0x000028D4
   SCB : 0x0AC5BD5B
   Channel: 0x00007fffed817200
IPSEC: Completed inbound VPN context, SPI 0x7AD72E0D
   VPN handle: 0x000000000004174
IPSEC: Updating outbound VPN context 0x000028D4, SPI 0x8C14FD70
   Flags: 0x00000205
   SA : 0x00007fffe1c75c00
   SPI : 0x8C14FD70
  MTU : 1500 bytes
  VCID : 0x0000000
```

```
Peer : 0x00004174
  SCB : 0x0AC609F9
  Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
  VPN handle: 0x000000000028d4
IPSEC: Completed outbound inner rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c763d0
IPSEC: Completed outbound outer SPD rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c76a00
IPSEC: New inbound tunnel flow rule, SPI 0x7AD72E0D
  Src addr: 10.1.1.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 1701
    Lower: 1701
    Op : equal
  Dst ports
    Upper: 1701
    Lower: 1701
    Op : equal
   Protocol: 17
  Use protocol: true
  SPI: 0x0000000
  Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x7AD72E0D
  Rule ID: 0x00007fffe13aba90
IPSEC: New inbound decrypt rule, SPI 0x7AD72E0D
  Src addr: 10.1.1.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
   Protocol: 50
  Use protocol: true
   SPI: 0x7AD72E0D
  Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x7AD72E0D
  Rule ID: 0x00007fffe1c77420
IPSEC: New inbound permit rule, SPI 0x7AD72E0D
  Src addr: 10.1.1.2
  Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
   Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x7AD72E0D
   Use SPI: true
```

```
IPSEC: Completed inbound permit rule, SPI 0x7AD72E0D
Rule ID: 0x00007fffe13abb80
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Pitcher: received
KEY_UPDATE, spi 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P2 rekey timer:
3420 seconds.
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

#### PHASE 2 COMPLETED

(msgid=00000001)
May 18 04:17:18 [IKEv1]IKEQM\_Active() Add L2TP classification rules: ip <10.1.1.2> mask
<0xFFFFFFF> port <1701>
May 18 04:17:21 [IKEv1]Group = DefaultRAGroup,

### Username = test, IP = 10.1.1.2, Adding static route for client address: 192.168.1.1

Certaines des erreurs VPN courantes sur le client Windows sont affichées dans ce tableau

« Error Code	Solution possible
691	S'assurer que le nom d'utilisateur et le mot de passe saisis sont corrects
789,835	S'assurer que la clé pré-partagée configurée sur la machine cliente est identique à celle de l'AS
800	1. Assurez-vous que le type de VPN est défini sur « L2TP (Layer 2 Tunneling Protocol)"
	2. Assurez-vous que la clé pré-partagée a été configurée correctement
809	Assurez-vous que les ports UDP 500 et 4500 (si le client ou le serveur est derrière le périphériq
	NAT) et que le trafic ESP n'a pas été bloqué

## Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance
- Support et documentation techniques Cisco Systems