

Configuration d'IPSec entre deux routeurs et un client VPN Cisco 4.x

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Cisco VPN 2611](#)

[Cisco VPN 3640](#)

[Vérifier les numéros de la séquence de la carte de chiffrement](#)

[Dépannez](#)

[Dépannage des commandes](#)

[Informations connexes](#)

[Introduction](#)

Ce document démontre comment configurer IPSec entre deux routeurs Cisco et le client VPN Cisco 4.x. Cisco IOS® versions 12.2(8)T ou ultérieures prend en charge les connexions des clients VPN Cisco versions 3.x et ultérieures.

Référez-vous à [configurer un pair dynamique et des clients vpn d'entre réseaux locaux de routeur d'IPsec](#) afin de se renseigner plus sur le scénario où une extrémité du tunnel L2L est assignée une adresse IP dynamiquement par l'autre extrémité.

[Conditions préalables](#)

[Conditions requises](#)

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Un groupe d'adresses à assigner pour IPSec
- Un groupe a appelé **3000clients** avec une clé pré-partagée de **cisco123** pour les clients vpn
- Le groupe et l'authentification de l'utilisateur est fait localement sur le routeur pour les clients vpn.
- Le paramètre de NO--**Xauth** est utilisé sur la commande de **clé d'ISAKMP** pour le tunnel entre

réseaux locaux.

Composants utilisés

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

- Routeurs qui exécutent le Logiciel Cisco IOS version 2.2(8)T. **Remarque:** Ce document a été récemment testé avec le Logiciel Cisco IOS version 12.3(1). Aucune modification n'est exigée.
- Client VPN Cisco pour la version 4.x de Windows (tout client 3.x VPN et travaux postérieurs).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

La sortie de la commande de **show version** sur le routeur est affichée dans cette sortie.

```
vpn2611#show version Cisco Internetwork Operating System Software IOS (tm) C2600 Software
(C2600-JK9O3S-M), Version 12.2(8)T, RELEASE SOFTWARE (fc2) TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc. Compiled Thu 14-Feb-02 16:50 by ccai Image text-
base: 0x80008070, data-base: 0x81816184 ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE
SOFTWARE (fc1) vpn2611 uptime is 1 hour, 15 minutes System returned to ROM by reload System
image file is "flash:c2600-jk9o3s-mz.122-8.T" cisco 2611 (MPC860) processor (revision 0x203)
with 61440K/4096K bytes of memory. Processor board ID JAD04370EEG (2285146560) M860 processor:
part number 0, mask 49 Bridging software. X.25 software, Version 3.0.0. SuperLAT software
(copyright 1990 by Meridian Technology Corp). TN3270 Emulation software. 2 Ethernet/IEEE 802.3
interface(s) 1 Serial network interface(s) 32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write) Configuration register is 0x2102
```

Conventions

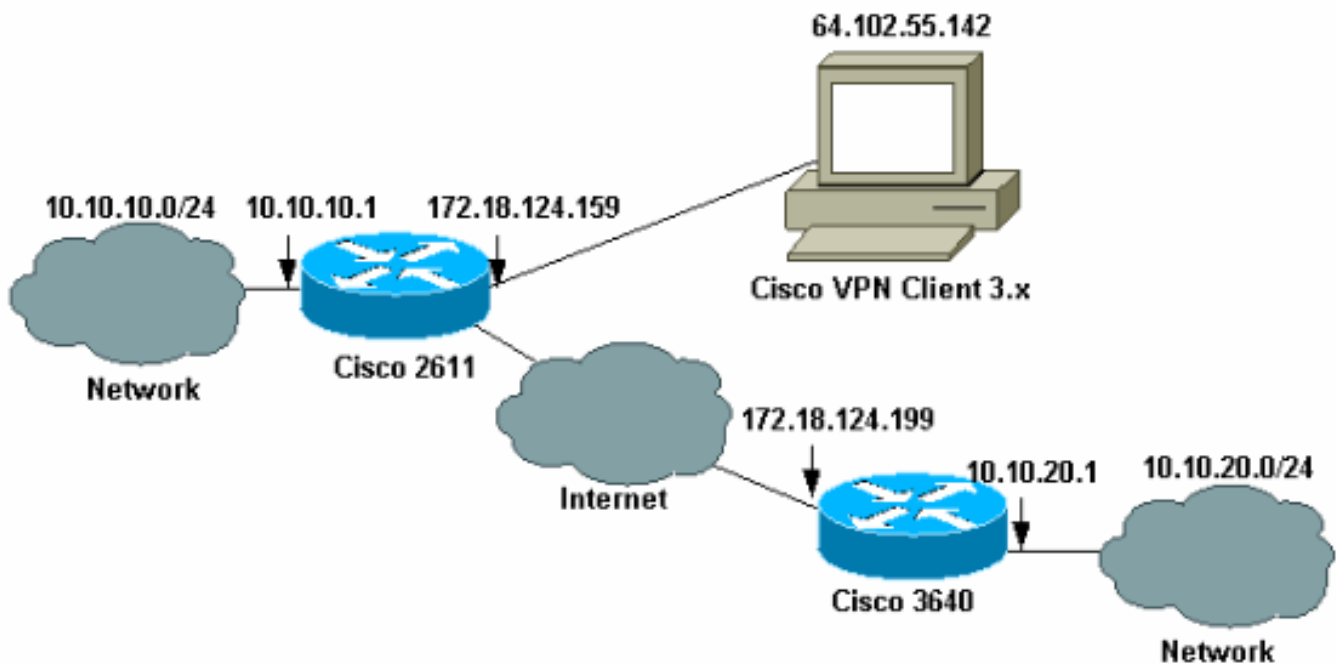
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise cette configuration du réseau.



Remarque: Les adresses IP dans cet exemple ne sont pas routable en Internet global parce qu'elles sont des adresses IP privées dans un réseau des travaux pratiques.

Configurations

Configurez le routeur de Cisco 2611

Routeur de Cisco 2611

```
vpn2611#show run Building configuration... Current
configuration : 2265 bytes ! version 12.2 service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname vpn2611 ! !---
Enable AAA for user authentication !--- and group
authorization. aaa new-model ! ! !--- In order to enable
X-Auth for user authentication, !--- enable the aaa
authentication commands. aaa authentication login
userauthen local !--- In order to enable group
authorization, enable !--- the aaa authorization
commands. aaa authorization network groupauthor local
aaa session-id common ! !--- For local authentication of
the IPSec user, !--- create the user with a password.
username cisco password 0 cisco ip subnet-zero ! ! ! ip
audit notify log ip audit po max-events 100 ! !---
Create an Internet Security Association and !--- Key
Management Protocol (ISAKMP) !--- policy for Phase 1
negotiations for the VPN 3.x Clients. crypto isakmp
policy 3 encr 3des authentication pre-share group 2 ! !-
-- Create an ISAKMP policy for Phase 1 !--- negotiations
for the LAN-to-LAN tunnels. crypto isakmp policy 10 hash
md5 authentication pre-share !--- Specify the PreShared
key for the LAN-to-LAN tunnel. !--- Make sure that you
use the !--- no-xauth parameter with your ISAKMP key.
crypto isakmp key cisco123 address 172.18.124.199 no-
xauth ! !--- Create a group that is used to !--- specify
the WINS, DNS servers' address !--- to the client, along
with the pre-shared !--- key for authentication. crypto
```

```

isakmp client configuration group 3000client key
cisco123 dns 10.10.10.10 wins 10.10.10.20 domain
cisco.com pool ippool ! ! !--- Create the Phase 2 Policy
for actual data encryption. crypto ipsec transform-set
myset esp-3des esp-md5-hmac ! !--- Create a dynamic map
and apply !--- the transform set that was created
earlier. crypto dynamic-map dynmap 10 set transform-set
myset ! ! !--- Create the actual crypto map, and !---
apply the AAA lists that were created !--- earlier. Also
create a new instance for your !--- LAN-to-LAN tunnel.
Specify the peer IP address, !--- transform set, and an
Access Control List (ACL) for this !--- instance. crypto
map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor crypto map clientmap client configuration
address respond crypto map clientmap 1 ipsec-isakmp set
peer 172.18.124.199 set transform-set myset match
address 100 crypto map clientmap 10 ipsec-isakmp dynamic
dynmap ! ! fax interface-type fax-mail mta receive
maximum-recipients 0 ! ! !--- Apply the crypto map on
the outside interface. interface Ethernet0/0 ip address
172.18.124.159 255.255.255.0 half-duplex crypto map
clientmap ! interface Serial0/0 no ip address shutdown !
interface Ethernet0/1 ip address 10.10.10.1
255.255.255.0 no keepalive half-duplex ! ! !--- Create a
pool of addresses to be !--- assigned to the VPN
Clients. ip local pool ippool 14.1.1.100 14.1.1.200 ip
classless ip route 0.0.0.0 0.0.0.0 172.18.124.1 ip http
server ip pim bidir-enable ! ! !--- Create an ACL for
the traffic !--- to be encrypted. In this example, !---
the traffic from 10.10.10.0/24 to 10.10.20.0/24 !--- is
encrypted. access-list 100 permit ip 10.10.10.0
0.0.0.255 10.10.20.0 0.0.0.255 ! ! snmp-server community
foobar RO call rsvp-sync ! ! mgcp profile default !
dial-peer cor custom ! ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 ! ! end

```

[Configurez le routeur 3640](#)

Routeur Cisco 3640

```

vpn3640#show run Building configuration... Current
configuration : 1287 bytes ! ! Last configuration change
at 13:47:37 UTC Wed Mar 6 2002 ! version 12.2 service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname vpn3640 ! ! ip
subnet-zero ip cef ! !--- Create an ISAKMP policy for
Phase 1 !--- negotiations for the LAN-to-LAN tunnels.
crypto isakmp policy 10 hash md5 authentication pre-
share ! !--- Specify the PreShared key for the LAN-to-LAN
!--- tunnel. You do not have to add the !--- X-Auth
parameter, as this !--- router does not do Cisco Unity
Client IPsec !--- authentication. crypto isakmp key
cisco123 address 172.18.124.159 ! ! !--- Create the
Phase 2 Policy for actual data encryption. crypto ipsec
transform-set myset esp-3des esp-md5-hmac ! !--- Create
the actual crypto map. Specify !--- the peer IP address,
transform !--- set, and an ACL for this instance. crypto
map mymap 10 ipsec-isakmp set peer 172.18.124.159 set
transform-set myset match address 100 ! call RSVP-sync !
! ! !--- Apply the crypto map on the outside interface.
interface Ethernet0/0 ip address 172.18.124.199
255.255.255.0 half-duplex crypto map mymap ! interface

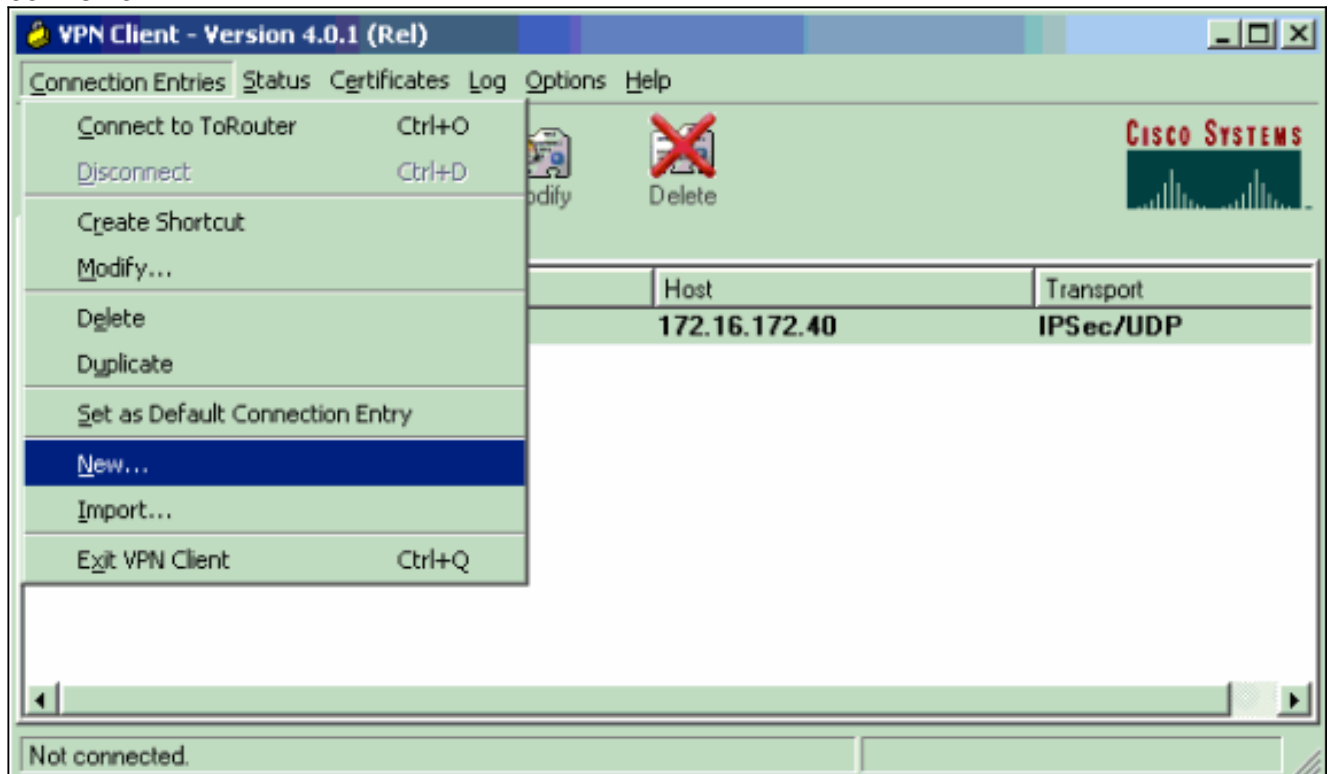
```

```
Ethernet0/1 ip address 10.10.20.1 255.255.255.0 half-  
duplex ! ip classless ip route 0.0.0.0 0.0.0.0  
172.18.124.1 ip http server ip pim bidir-enable ! !---  
Create an ACL for the traffic to !--- be encrypted. In  
this example, !--- the traffic from 10.10.20.0/24 to  
10.10.10.0/24 !--- is encrypted. access-list 100 permit  
ip 10.10.20.0 0.0.0.255 10.10.10.0 0.0.0.255 snmp-server  
community foobar RO ! dial-peer cor custom ! ! line con  
0 exec-timeout 0 0 line aux 0 line vty 0 4 login ! end
```

[Configurez le client vpn 4.x](#)

Suivez ces étapes afin de configurer le Client VPN Cisco 4.x.

1. Lancez le client vpn, et puis cliquez sur New afin de créer une nouvelle connexion.



2. Entrez les informations nécessaires, et cliquez sur la **sauvegarde** une fois

VPN Client | Create New VPN Connection Entry

Connection Entry:

Description:

Host:

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication

Name:

Password:

Confirm Password:

Certificate Authentication

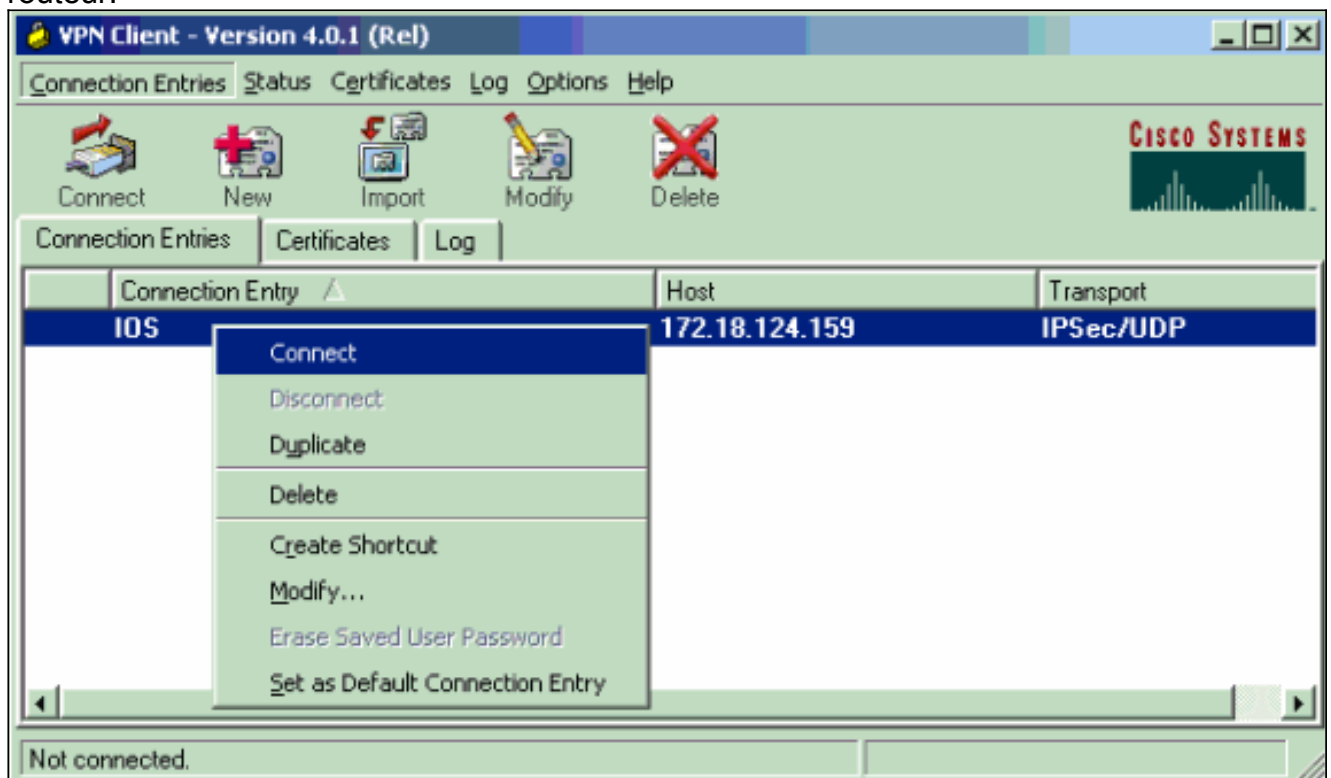
Name:

Send CA Certificate Chain

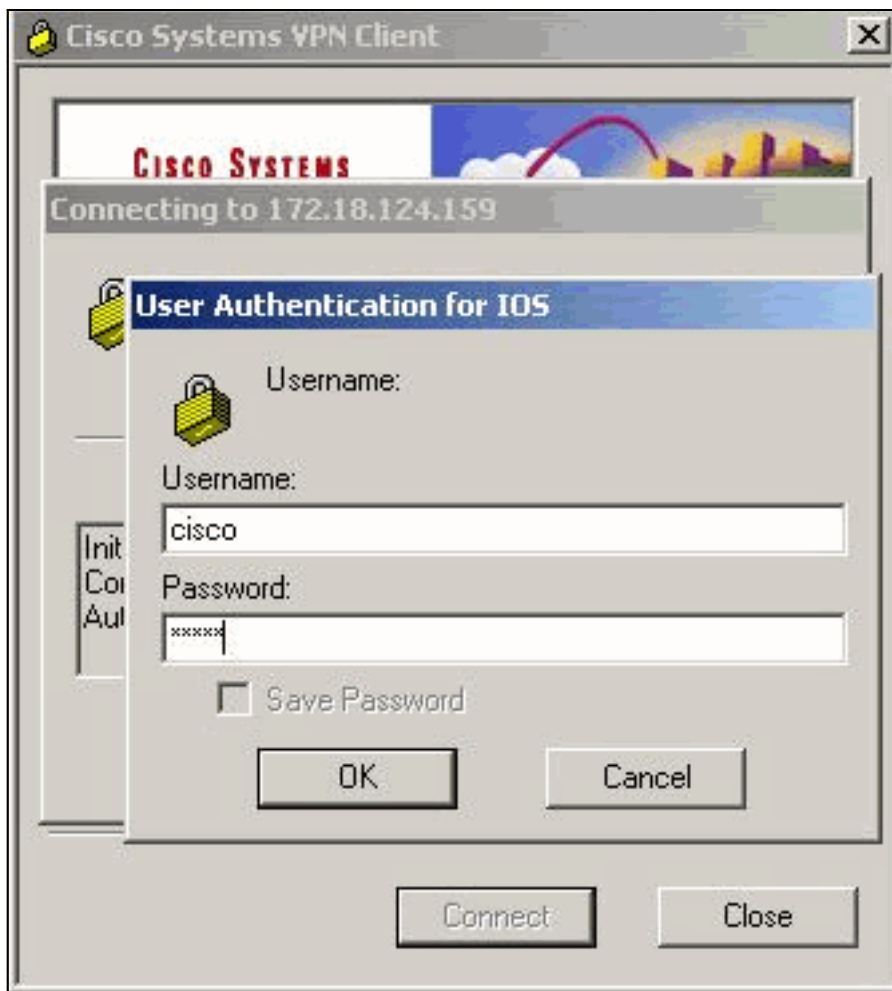
Erase User Password | Save | Cancel

terminé.

3. Cliquez avec le bouton droit sur l'entrée de création récente de connexion, et le clic **se connectent** afin de se connecter au routeur.



4. Pendant les négociations IPSecs, vous êtes incité pour un nom d'utilisateur et mot de



passee.

5. La fenêtre affiche les messages qui lisent « des profils de Sécurité de négociation » et « votre lien est maintenant sécurisé. »

Vérifiez

Cette section fournit les informations qui vous aident à confirmer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) ([clients enregistrés](#) uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Cisco VPN 2611

```
vpn2611#show crypto isakmp sa dst src state conn-id slot 172.18.124.159 172.18.124.199 QM_IDLE 5
0 !--- For the LAN-to-LAN tunnel peer. 172.18.124.159 64.102.55.142 QM_IDLE 6 0 !--- For the
Cisco Unity Client tunnel peer. vpn2611#show crypto ipsec sa interface: Ethernet0/0 Crypto map
tag: clientmap, local addr. 172.18.124.159 protected vrf: local ident (addr/mask/prot/port):
(10.10.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port):
(10.10.20.0/255.255.255.0/0/0) current_peer: 172.18.124.199:500 !--- For the LAN-to-LAN tunnel
peer. PERMIT, flags={origin_is_acl,} #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4 #pkts
decaps: 4, #pkts decrypt: 4, #pkts verify 4 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0
local crypto endpt.: 172.18.124.159, remote crypto endpt.: 172.18.124.199 path mtu 1500, media
mtu 1500 current outbound spi: 892741BC inbound esp sas: spi: 0x7B7B2015(2071666709) transform:
esp-3des esp-md5-hmac , in use settings = {Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto
map: clientmap sa timing: remaining key lifetime (k/sec): (4607999/1182) IV size: 8 bytes replay
detection support: Y inbound ah sas: inbound pcp sas: outbound ESP sas: spi:
0x892741BC(2301051324) transform: esp-3des esp-md5-hmac , in use settings = {Tunnel, } slot: 0,
```



```

conn id: 2001, flow_id: 2, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4607999/1182) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound PCP sas:
protected vrf: local ident (addr/mask/prot/port): (172.18.124.159/255.255.255.255/0/0) remote
ident (addr/mask/prot/port): (14.1.1.106/255.255.255.255/0/0) current_peer: 64.102.55.142:500 !-
-- For the Cisco Unity Client tunnel peer. PERMIT, flags={} #pkts encaps: 0, #pkts encrypt: 0,
#pkts digest 0 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0 local crypto endpt.: 172.18.124.159, remote crypto endpt.:
64.102.55.142 path mtu 1500, media mtu 1500 current outbound spi: 81F39EFA inbound ESP sas: spi:
0xC4483102(3293065474) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2002, flow_id: 3, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4608000/3484) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound PCP sas:
outbound ESP sas: spi: 0x81F39EFA(2180226810) transform: esp-3des esp-md5-hmac , in use settings
={Tunnel, } slot: 0, conn id: 2003, flow_id: 4, crypto map: clientmap sa timing: remaining key
lifetime (k/sec): (4608000/3484) IV size: 8 bytes replay detection support: Y outbound ah sas:
outbound PCP sas: protected vrf: local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote
ident (addr/mask/prot/port): (14.1.1.106/255.255.255.255/0/0) current_peer: 64.102.55.142:500 !-
-- For the Cisco Unity Client tunnel peer. PERMIT, flags={} #pkts encaps: 4, #pkts encrypt: 4,
#pkts digest 4 #pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0 local crypto endpt.: 172.18.124.159, remote crypto endpt.:
64.102.55.142 path mtu 1500, media mtu 1500 current outbound spi: B7F84138 inbound ESP sas: spi:
0x5209917C(1376358780) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2004, flow_id: 5, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4607998/3474) IV size: 8 bytes replay detection support: Y spi: 0xDE6C99C0(3731659200)
transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2006, flow_id:
7, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4607998/3493) IV size: 8
bytes replay detection support: Y inbound ah sas: inbound PCP sas: outbound ESP sas: spi:
0x58886878(1485334648) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2005, flow_id: 6, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4608000/3474) IV size: 8 bytes replay detection support: Y spi: 0xB7F84138(3086500152)
transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2007, flow_id:
8, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4607999/3486) IV size: 8
bytes replay detection support: Y outbound ah sas: outbound PCP sas: vpn2611#show crypto engine
connection active ID Interface IP-Address State Algorithm Encrypt Decrypt 5 Ethernet0/0
172.18.124.159 set HMAC_MD5+DES_56_CB 0 0 6 Ethernet0/0 172.18.124.159 set HMAC_SHA+3DES_56_C 0
0 2000 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 4 2001 Ethernet0/0 172.18.124.159 set
HMAC_MD5+3DES_56_C 4 0 2002 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 0 2003
Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 0 2004 Ethernet0/0 172.18.124.159 set
HMAC_MD5+3DES_56_C 0 9 2005 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 0 2006
Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 79 2007 Ethernet0/0 172.18.124.159 set
HMAC_MD5+3DES_56_C 4 0 vpn2611#

```

Cisco VPN 3640

```

vpn3640#show crypto isakmp sa DST src state conn-id slot 172.18.124.159 172.18.124.199 QM_IDLE 4
0 !--- For the LAN-to-LAN tunnel peer. vpn3640#show crypto ipsec sa interface: Ethernet0/0
Crypto map tag: mymap, local addr. 172.18.124.199 protected vrf: local ident
(addr/mask/prot/port): (10.10.20.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port):
(10.10.10.0/255.255.255.0/0/0) current_peer: 172.18.124.159:500 !--- For the LAN-to-LAN tunnel
peer. PERMIT, flags={origin_is_acl,} #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4 #pkts
decaps: 4, #pkts decrypt: 4, #pkts verify 4 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0 #send errors 11, #recv errors
0 local crypto endpt.: 172.18.124.199, remote crypto endpt.: 172.18.124.159 path mtu 1500, media
mtu 1500 current outbound spi: 7B7B2015 inbound ESP sas: spi: 0x892741BC(2301051324) transform:
esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 940, flow_id: 1, crypto
map: mymap sa timing: remaining key lifetime (k/sec): (4607998/1237) IV size: 8 bytes replay
detection support: Y inbound ah sas: inbound PCP sas: outbound ESP sas: spi:
0x7B7B2015(2071666709) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 941, flow_id: 2, crypto map: mymap sa timing: remaining key lifetime(k/sec):
(4607999/1237) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound PCP sas:
vpn3640# show crypto engine connection active ID Interface IP-Address State Algorithm Encrypt
Decrypt 4 <none> <none> set HMAC_MD5+DES_56_CB 0 0 940 Ethernet0/0 172.18.124.199 set
HMAC_MD5+3DES_56_C 0 4 941 Ethernet0/0 172.18.124.199 set HMAC_MD5+3DES_56_C 4 0

```


Vérifier les numéros de la séquence de la carte de chiffrement

Si des homologues statiques et dynamiques sont configurés sur la même carte de chiffrement, l'ordre des entrées dans la carte de chiffrement est très important. Le numéro de séquence de l'entrée dynamique de la carte de chiffrement **doit être** plus élevé que toutes les autres entrées statiques de la carte de chiffrement. Si les entrées statiques portent un numéro plus élevé que l'entrée dynamique, les connexions avec ces homologues échouent.

Voici un exemple de carte de chiffrement correctement numérotée qui contient une entrée statique et une entrée dynamique. Notez que l'entrée dynamique a le numéro de séquence le plus élevé et que de la place a été laissée pour ajouter des entrées statiques supplémentaires :

```
crypto dynamic-map dynmap 10
set transform-set myset
crypto map clientmap 1 ipsec-isakmp
set peer 172.18.124.199
set transform-set myset
match address 100
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
```

Dépannez

Cette section fournit les informations qui aident à dépanner votre configuration.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) ([clients enregistrés](#) uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque: Référez-vous aux [informations importantes sur des commandes de debug](#) avant que vous émettiez des commandes de **débogage**.

- **debug crypto ipsec** : affiche des événements IPsec. *Le forme no de* cette commande désactive la sortie de débogage.
- **debug crypto isakmp**—Affichage de messages d'événements IKE. *Le forme no de* cette commande désactive la sortie de débogage.
- **debug crypto engine** — Affiche des informations tel que laquelle concerne le moteur de chiffrement, quand le logiciel de Cisco IOS exécute des opérations de cryptage ou de déchiffrement.

Informations connexes

- [Page de support pour Protocole IKE/Négociation IPsec](#)
- [Support et documentation techniques - Cisco Systems](#)