Exemple de configuration du tunnel IPsec entre routeur IOS et client VPN Cisco 4.x pour Windows avec authentification utilisateur TACACS+

Contenu

Introduction

Ce document décrit comment configurer une connexion d'IPsec entre un routeur et le client du réseau privé virtuel de Cisco (VPN) 4.x avec le Terminal Access Controller Access Control System Plus (TACACS+) pour l'authentification de l'utilisateur. Les versions de version de logiciel 12.2(8)T et ultérieures de Cisco IOS® prennent en charge des connexions du Client VPN Cisco 4.x. Le client vpn 4.x utilise la stratégie du groupe 2 de Diffie-Hellman (D-H). Les commandes enables de **stratégie # de groupe 2 d'ISAKMP les** clients 4.x à connecter.

Ce document affiche l'authentification sur le serveur TACACS+ avec l'autorisation, telle que des affectations de Windows Internet Naming Service (WINS) et de service de nom de domaine (DN), exécutées localement par le routeur.

Référez-vous à configurer le Client VPN Cisco 3.x pour Windows à l'IOS utilisant l'authentification étendue locale afin de se renseigner plus sur le scénario où l'authentification de l'utilisateur se produit localement dans le routeur Cisco IOS.

Référez-vous à la configuration d'IPSec entre un routeur Cisco IOS et un Client VPN Cisco 4.x pour Windows utilisant le RAYON pour l'authentification de l'utilisateur afin de se renseigner plus sur le scénario où l'authentification de l'utilisateur se produit extérieurement avec le protocole

RADIUS.

Conditions préalables

Conditions requises

Assurez-vous de répondre à ces exigences avant d'essayer cette configuration :

- Un groupe d'adresses à assigner pour IPsec
- Un groupe a nommé le « vpngroup » avec un mot de passe de "cisco123"
- Authentification de l'utilisateur sur un serveur TACACS+

Composants utilisés

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

- Client VPN Cisco pour la version 4.0.2D de Windows (n'importe quel client 3.x VPN ou plus tard devrait travailler.)
- Cisco Secure pour la version 3.0 de Windows (n'importe quel serveur TACACS+ devrait travailler)
- La version 12.2(8)T1 de routeur du Cisco IOS 1710 a chargé avec le positionnement de caractéristique d'IPsecLa sortie de la commande de **show version** sur le routeur est affichée ici.

```
1710#show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1710-K9O3SY-M),
   Version 12.2(8)T1, RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 30-Mar-02 13:30 by ccai
Image text-base: 0x80008108, data-base: 0x80C1E054

ROM: System Bootstrap, Version 12.2(1r)XE1, RELEASE SOFTWARE (fc1)

1710 uptime is 1 week, 6 days, 22 hours, 30 minutes
System returned to ROM by reload
System image file is "flash:c1710-k9o3sy-mz.122-8.T1"

cisco 1710 (MPC855T) processor (revision 0x200)
   with 27853K/4915K bytes of memory.
Processor board ID JAD052706CX (3234866109), with hardware revision 0000
MPC855T processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 Virtual Private Network (VPN) Module(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

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.

Conventions

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

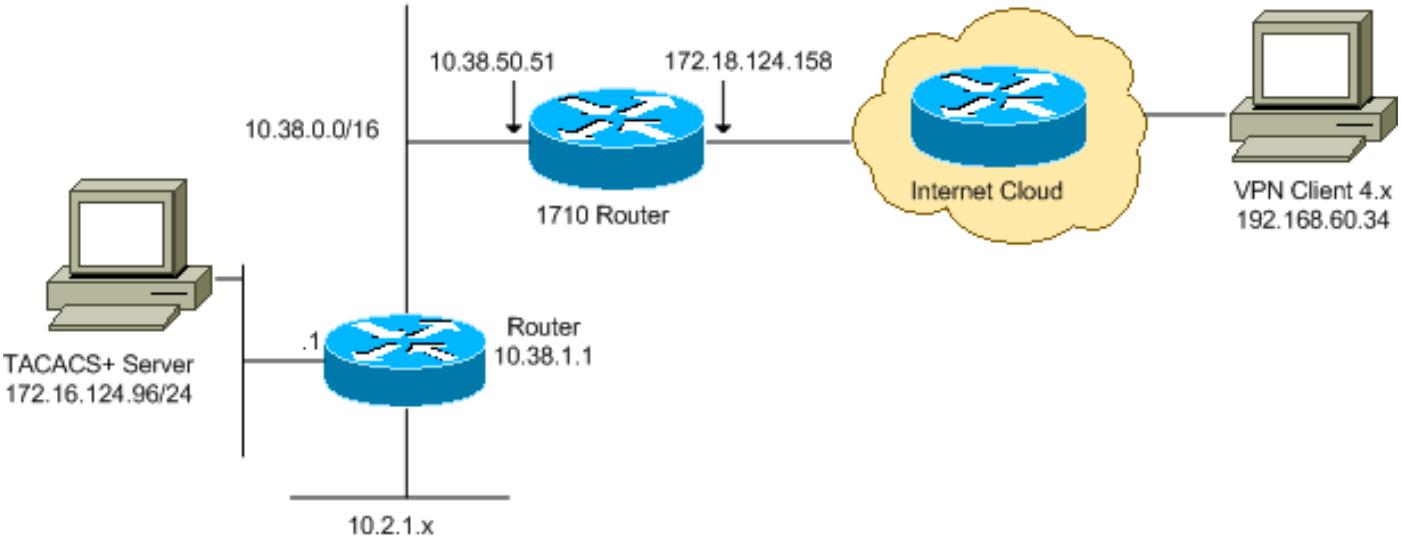
Configurez

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

Remarque: Utilisez l'outil de recherche de commande (réservé aux clients inscrits) pour plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque: 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.

Configurations

Ce document utilise les configurations suivantes :

- Routeur Cisco 1710
- Serveur TACACS+
- Client vpn 4.x
- transmission tunnel partagée

Routeur Cisco 1710

Routeur Cisco 1710

```
1710#show run
Building configuration...

Current configuration : 1884 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1710
!
!--- Enable authentication, authorization and accounting
(AAA) !--- for user authentication and group
authorization. aaa new-model
!
!--- In order to enable extended authentication (Xauth)
for user authentication, !--- enable the aaa
authentication commands. !--- The group TACACS+ command
specifies TACACS+ user authentication.

aaa authentication login userauthen group tacacs+
!--- In order to enable group authorization, !--- enable
the aaa authorization commands.

aaa authorization network groupauthor local
!
!
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. crypto isakmp policy 3
encr 3des
authentication pre-share
group 2
!
!--- Create a group in order to specify the !--- WINS
and DNS server addresses to the VPN Client, !--- along
with the pre-shared key for authentication. crypto
isakmp client configuration group vpngroup
key cisco123
dns 10.2.1.10
wins 10.2.1.20
domain cisco.com
pool ippool
!
!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-sha-hmac
!

!--- Create a dynamic map, and !--- apply the transform
set that was previously created. crypto dynamic-map
dynmap 10
set transform-set myset
!
```

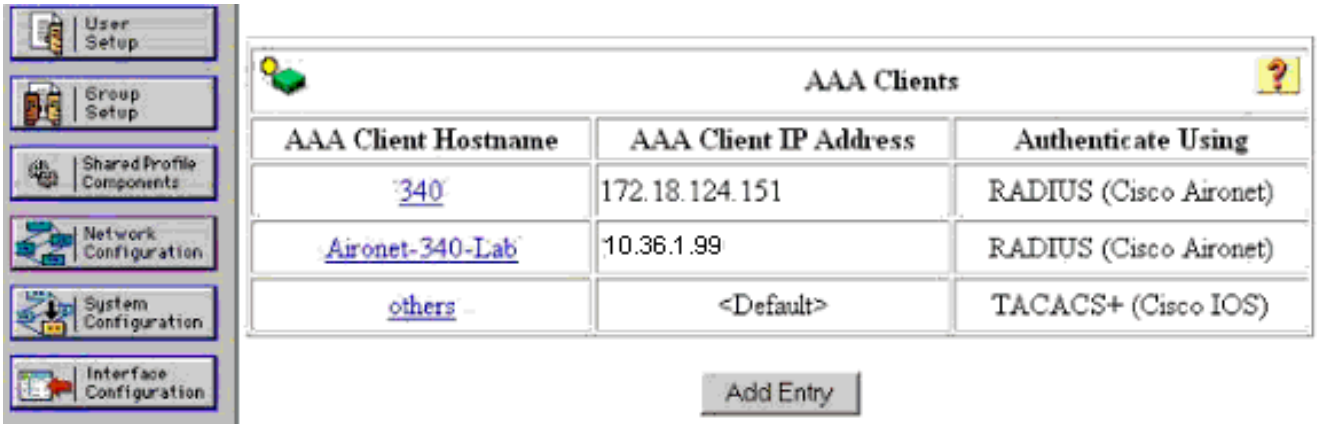
```
!--- Create the actual crypto map, !--- and apply the
AAA lists that were created earlier. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
!
!--- Apply the crypto map on the outside interface.
interface FastEthernet0
ip address 172.18.124.158 255.255.255.0
crypto map clientmap
!
interface Ethernet0
ip address 10.38.50.51 255.255.0.0
!

!--- Create a pool of addresses to be assigned to the
VPN Clients. ip local pool ippool 10.1.1.100 10.1.1.200
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip route 172.16.124.0 255.255.255.0 10.38.1.1
ip route 10.2.1.0 255.255.255.0 10.38.1.1
ip http server
ip pim bidir-enable
!
!
!
!--- Specify the IP address of the TACACS+ server, !---
along with the TACACS+ shared secret key. tacacs-server
host 172.16.124.96 key cisco123
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end
```

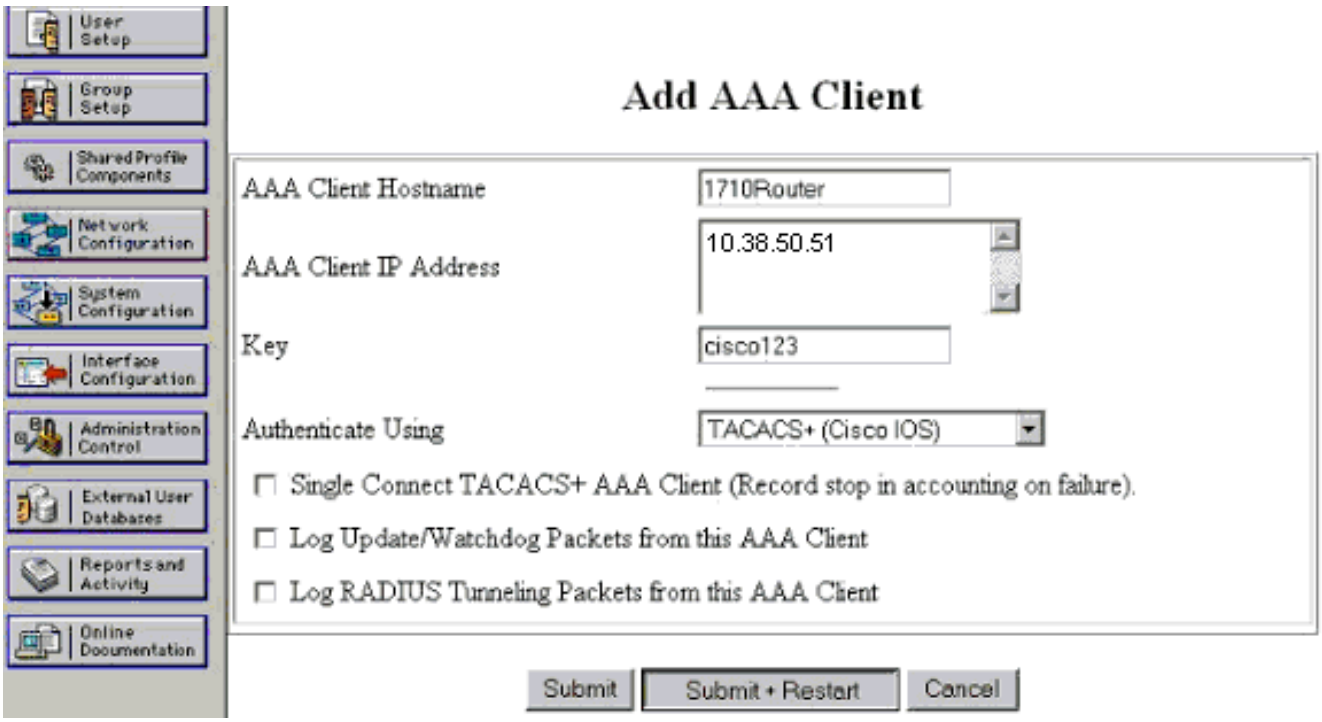
Serveur TACACS+

Afin de configurer le serveur TACACS+, terminez-vous ces étapes :

1. Cliquez sur Add l'**entrée** afin d'ajouter une entrée pour le routeur dans la base de données du serveur
   TACACS+.

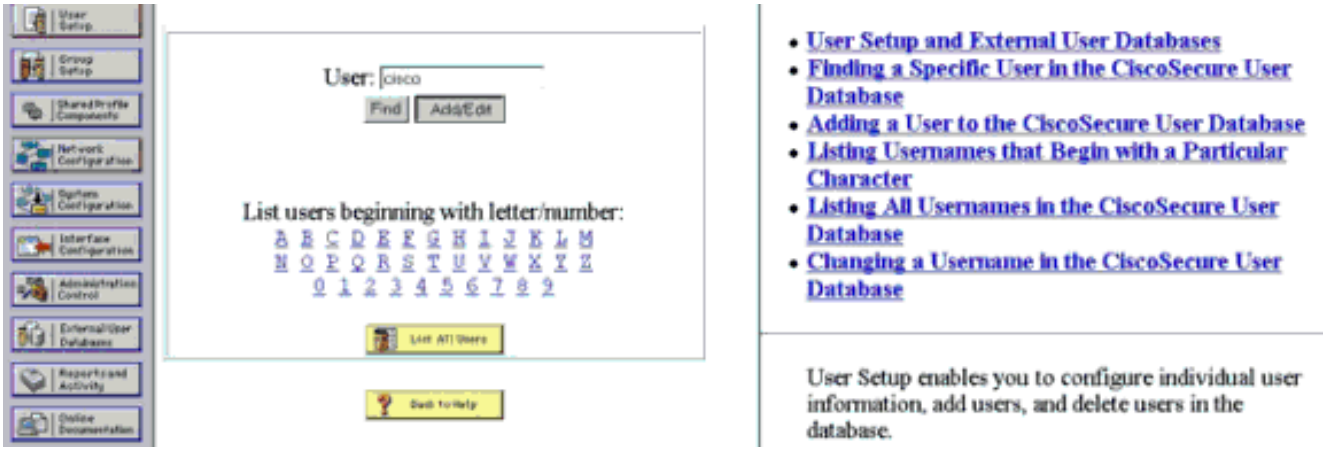


2. Àla page de client d'AAA d'ajouter, écrivez les informations de routeur suivant les indications de cette image
:

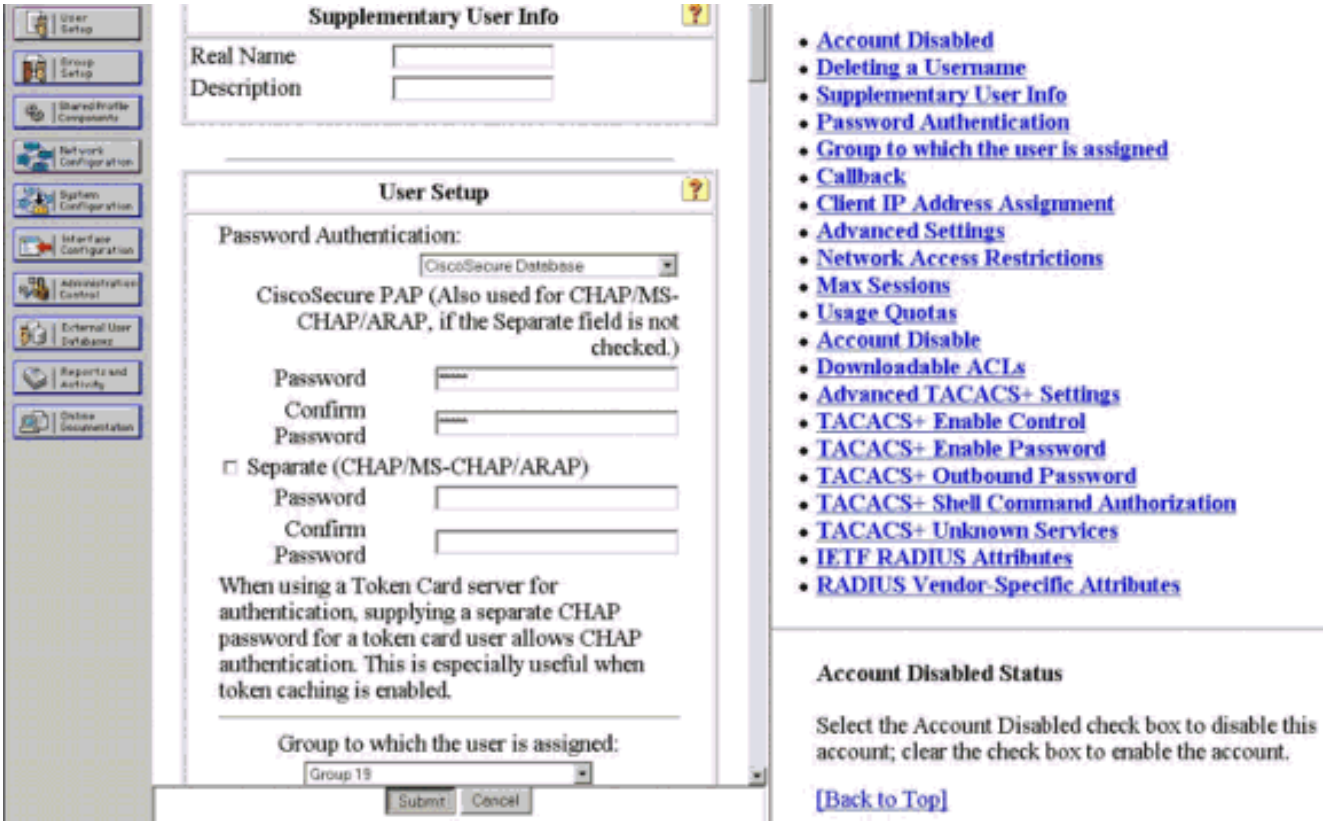


Dans le domaine d'adresse Internet de client d'AAA, écrivez un nom pour le routeur.Dans le champ IP Address de client d'AAA, entrez dans **10.38.50.51**.Dans la zone de tri, écrivez **cisco123** comme clé secrète partagée.De l'authentifier utilisant la liste déroulante, choisissez **TACACS+ (Cisco IOS)**, et cliquez sur Submit.

3. Dans le domaine d'utilisateur, écrivez le nom d'utilisateur pour l'utilisateur VPN dans la base de données Cisco Secure, et cliquez sur Add**/l'éditez**.Dans cet exemple, le nom d'utilisateur est
Cisco.



4. Sur la page suivante, entrez et confirmez le mot de passe pour l'utilisateur *Cisco*.Dans cet exemple, le mot de passe est également *Cisco*.

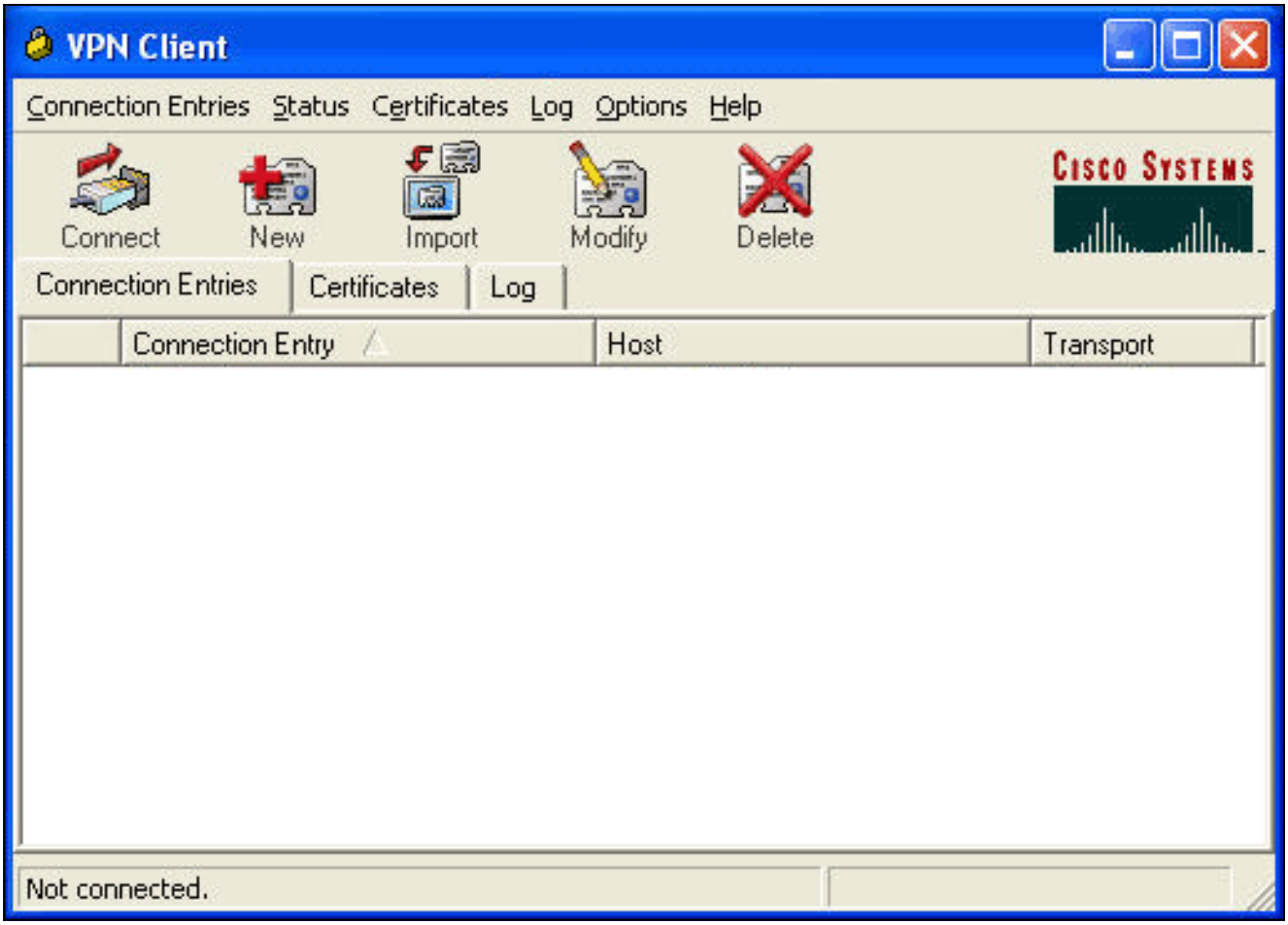


5. Si vous voulez tracer le compte utilisateur à un groupe, complet qui font un pas maintenant. Quand vous terminez, cliquez sur Submit.

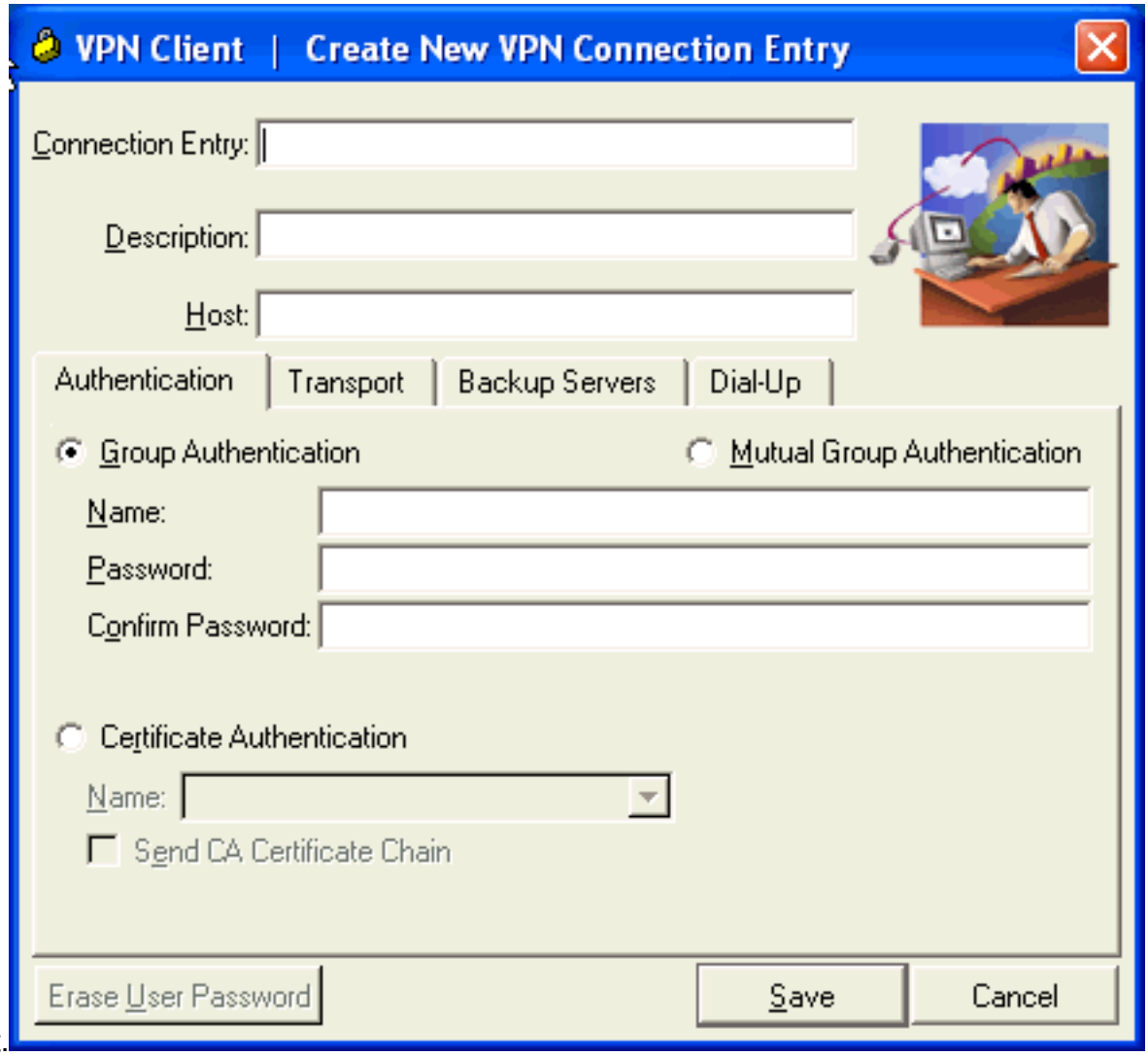
Client vpn 4.x

Afin de configurer le client vpn 4.x, terminez-vous ces étapes :

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

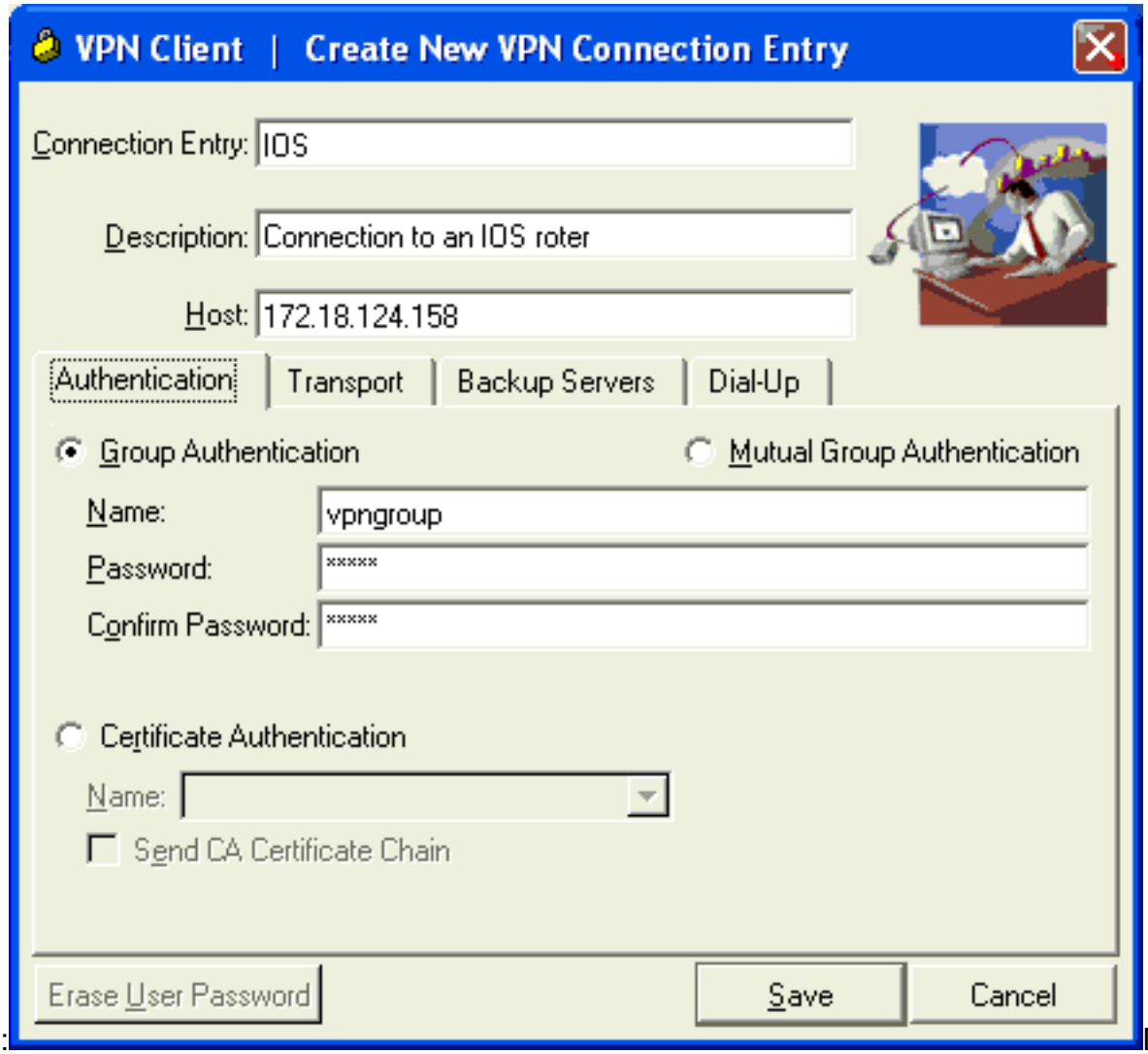


Le client vpn créent la nouvelle boîte de dialogue d'entrée de connexion VPN



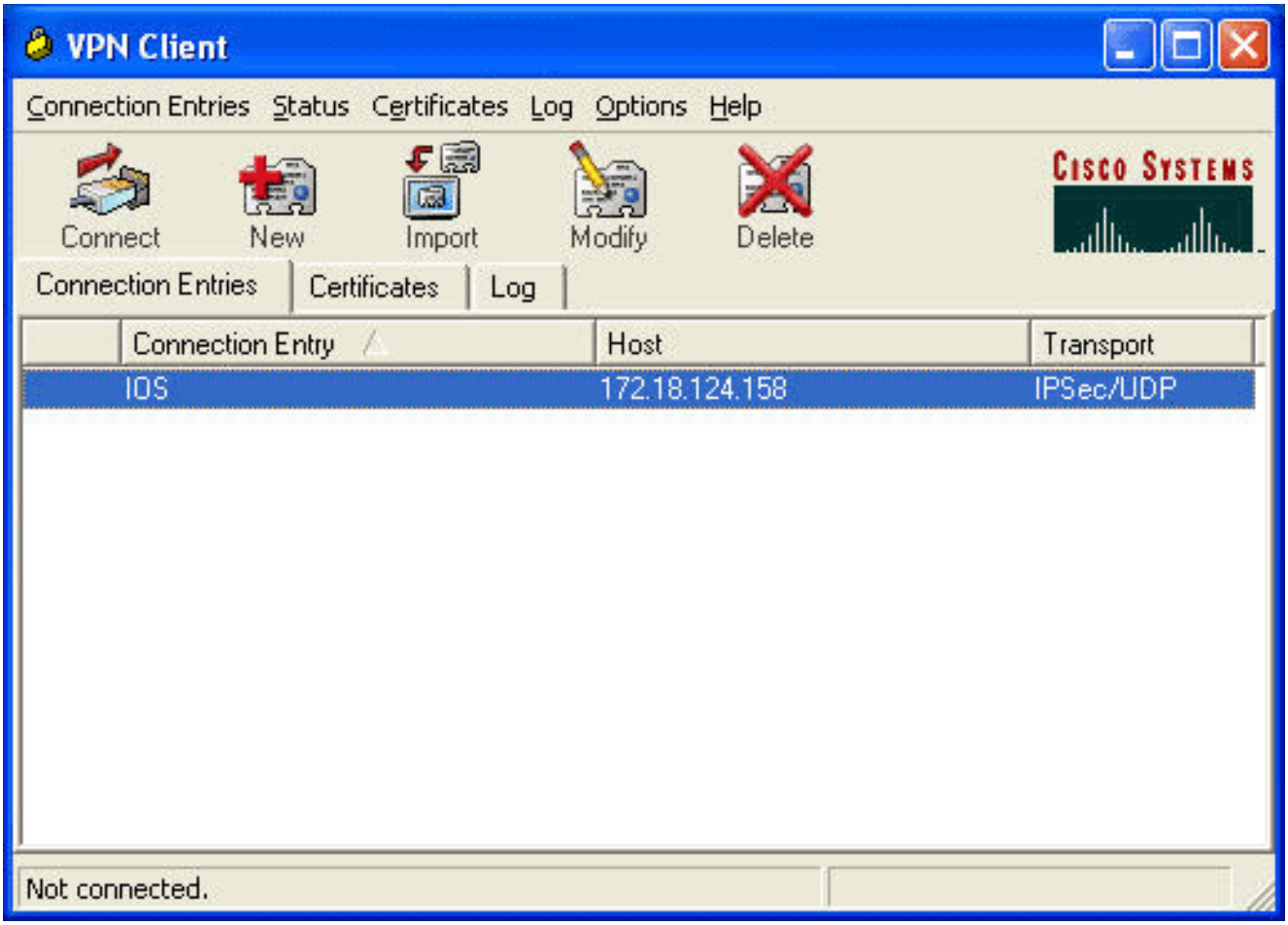
apparaît.

2. Dans la nouvelle boîte de dialogue d'entrée de connexion VPN de création, écrivez les informations de connexion suivant les indications de cette image



:Dans le domaine d'entrée de connexion, écrivez un nom pour la connexion.Dans la description et les champs Host, écrivez une description et l'adresse IP d'hôte pour l'entrée de connexion.Sur l'onglet d'authentification, cliquez sur la case d'option d'**authentification de groupe**, et entrez le nom et le mot de passe de l'utilisateur.**Sauvegarde de** clic afin de sauvegarder la connexion.

3. Dans la fenêtre de client vpn, sélectionnez l'entrée de connexion que vous avez créée, et le clic **se connectent** afin de se connecter au routeur.



4. Pendant qu'IPsec négocie, vous êtes incité pour un nom d'utilisateur et un mot de passe. Entrez un nom d'utilisateur et un mot de passe.La fenêtre affiche ces messages :« Profils de Sécurité de négociation. »« Votre lien est maintenant sécurisé. »

[transmission tunnel partagée]

Afin d'activer la Segmentation de tunnel pour les connexions VPN, veillez-vous pour configurer une liste de contrôle d'accès (ACL) sur le routeur. Dans cet exemple, la commande de la **liste d'accès 102** est associée avec le groupe pour des buts de partitionner la mise en tunnel, et le tunnel est formé aux réseaux 10.38.X.X /16 et 10.2.x.x. La circulation décryptée aux périphériques pas dans l'ACL 102 (par exemple, l'Internet).

```
access-list 102 permit ip 10.38.0.0 0.0.255.255 10.1.1.0 0.0.0.255
access-list 102 permit ip 10.2.0.0 0.0.255.255 10.1.1.0 0.0.0.255
```

Appliquez l'ACL sur les propriétés de groupe.

```
crypto isakmp client configuration group vpngroup
 key cisco123
 dns 10.2.1.10
 wins 10.2.1.20
 domain cisco.com
 pool ippool
 acl 102
```

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre

configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'outil Output Interpreter Tool (clients **enregistrés** seulement). Cet outil te permet pour visualiser une analyse de sortie de commande show.

```
1710#show crypto isakmp sa
dst             src             state          conn-id    slot
172.18.124.158  192.168.60.34   QM_IDLE              3       0


1710#show crypto ipsec sa

interface: FastEthernet0
Crypto map tag: clientmap, local addr. 172.18.124.158

local ident (addr/mask/prot/port): (172.18.124.158/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.1.1.114/255.255.255.255/0/0)
current_peer: 192.168.60.34
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.: 172.18.124.158, remote crypto endpt.: 192.168.60.34
path mtu 1500, media mtu 1500
current outbound spi: 8F9BB05F

inbound esp sas:
spi: 0x61C53A64(1640315492)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 200, flow_id: 1, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4608000/3294)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8F9BB05F(2409345119)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 201, flow_id: 2, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4608000/3294)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:


local ident (addr/mask/prot/port): (10.38.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.114/255.255.255.255/0/0)
current_peer: 192.168.60.34
PERMIT, flags={}
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
```

```
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#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.: 172.18.124.158, remote crypto endpt.: 192.168.60.34
path mtu 1500, media mtu 1500
current outbound spi: 8B57E45E

inbound esp sas:
spi: 0x89898D1A(2307493146)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 202, flow_id: 3, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/3452)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8B57E45E(2337793118)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 203, flow_id: 4, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/3452)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:


1710#show crypto engine connections active

ID   Interface      IP-Address      State  Algorithm           Encrypt  Decrypt
2    FastEthernet0  172.18.124.158  set    HMAC_SHA+3DES_56_C  0        0
200  FastEthernet0  172.18.124.158  set    HMAC_SHA+3DES_56_C  0        0
201  FastEthernet0  172.18.124.158  set    HMAC_SHA+3DES_56_C  0        0
202  FastEthernet0  172.18.124.158  set    HMAC_SHA+3DES_56_C  0        3
203  FastEthernet0  172.18.124.158  set    HMAC_SHA+3DES_56_C  3        0
```

Dépannez

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

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

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

- **debug crypto ipsec** — Affiche des informations de débogage sur les connexions IPSec.
- **debug crypto isakmp** — Les affichages mettent au point des informations sur des connexions

d'IPsec et affichent le premier ensemble d'attributs qui sont refusés en raison des incompatibilités sur les deux extrémités.

- **debug crypto engine** — Affiche des informations du moteur de chiffrement.
- **debug aaa authentication** — Affiche des informations sur l'authentification AAA/TACACS+.
- **autorisation de debug aaa** — Affiche des informations sur l'autorisation AAA/TACACS+.
- **debug tacacs** — Affiche des informations qui te permet pour dépanner la transmission entre le serveur TACACS+ et le routeur.

Journaux du routeur

```
1710#show debug
General OS:
TACACS access control debugging is on
AAA Authentication debugging is on
AAA Authorization debugging is on
Cryptographic Subsystem:
Crypto ISAKMP debugging is on
Crypto Engine debugging is on
Crypto IPSEC debugging is on


1710#
1w6d: ISAKMP (0:0): received packet from 192.168.60.34 (N) NEW SA
1w6d: ISAKMP: local port 500, remote port 500
1w6d: ISAKMP (0:2): (Re)Setting client xauth list userauthen and state
1w6d: ISAKMP: Locking CONFIG struct 0x8158B894 from
   crypto_ikmp_config_initialize_sa, count 2
1w6d: ISAKMP (0:2): processing SA payload. message ID = 0
1w6d: ISAKMP (0:2): processing ID payload. message ID = 0
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): vendor ID seems Unity/DPD but bad major
1w6d: ISAKMP (0:2): vendor ID is XAUTH
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): vendor ID is DPD
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): vendor ID is Unity
1w6d: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 3 policy
1w6d: ISAKMP: encryption 3DES-CBC
1w6d: ISAKMP: hash SHA
1w6d: ISAKMP: default group 2
1w6d: ISAKMP: auth XAUTHInitPreShared
1w6d: ISAKMP: life type in seconds
1w6d: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: ISAKMP (0:2): atts are acceptable. Next payload is 3
1w6d: CryptoEngine0: generate alg parameter
1w6d: CryptoEngine0: CRYPTO_ISA_DH_CREATE(hw)(ipsec)
1w6d: CRYPTO_ENGINE: Dh phase 1 status: 0
1w6d: ISAKMP (0:2): processing KE payload. message ID = 0
1w6d: CryptoEngine0: generate alg parameter
1w6d: CryptoEngine0: CRYPTO_ISA_DH_SHARE_SECRET(hw)(ipsec)
1w6d: ISAKMP (0:2): processing NONCE payload. message ID = 0
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1
1w6d: AAA/MEMORY: create_user (0x817F63F4) user='vpngroup' ruser='NULL' ds0=0
   port='ISAKMP-ID-AUTH' rem_addr='192.168.60.34' authen_type=NONE
   service=LOGIN priv=0 initial_task_id='0'
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT
```

```
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894):
   Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET
1w6d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(1472763894) user='vpngroup'
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): send AV service=ike
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): send AV protocol=ipsec
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): found list "groupauthor"
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): Method=LOCAL
1w6d: AAA/AUTHOR (1472763894): Post authorization status = PASS_ADD
1w6d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV service=ike
AAA/AUTHOR/IKE: Processing AV protocol=ipsec
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com
AAA/AUTHOR/IKE: Processing AV addr-pool*ippool
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV timeout*0
AAA/AUTHOR/IKE: Processing AV idletime*0
AAA/AUTHOR/IKE: Processing AV inacl*102
AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0
AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0
1w6d: CryptoEngine0: create ISAKMP SKEYID for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_SA_CREATE(hw)(ipsec)
1w6d: ISAKMP (0:2): SKEYID state generated
1w6d: ISAKMP (0:2): SA is doing pre-shared key authentication plux
   XAUTH using id type ID_IPV4_ADDR
1w6d: ISAKMP (2): ID payload
next-payload : 10
type : 1
protocol : 17
port : 500
length : 8
1w6d: ISAKMP (2): Total payload length: 12
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) AG_INIT_EXCH
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

1w6d: AAA/MEMORY: free_user (0x817F63F4) user='vpngroup'
   ruser='NULL' port='ISAK MP-ID-AUTH' rem_addr='192.168.60.34'
   authen_type=NONE service=LOGIN priv=0
1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) AG_INIT_EXCH
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): processing HASH payload. message ID = 0
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): processing NOTIFY INITIAL_CONTACT protocol 1
   spi 0, message ID = 0, sa = 81673884
1w6d: ISAKMP (0:2): Process initial contact, bring down
   existing phase 1 and 2 SA's
1w6d: ISAKMP (0:2): returning IP addr to the address pool: 10.1.1.113
1w6d: ISAKMP (0:2): returning address 10.1.1.113 to pool
1w6d: ISAKMP (0:2): peer does not do paranoid keepalives.

1w6d: ISAKMP (0:2): SA has been authenticated with 192.168.60.34
1w6d: CryptoEngine0: clear dh number for conn id 1
1w6d: CryptoEngine0: CRYPTO_ISA_DH_DELETE(hw)(ipsec)
1w6d: IPSEC(key_engine): got a queue event...
1w6d: IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
1w6d: IPSEC(key_engine_delete_sas): delete all SAs shared with 192.168.60.34
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
```

```
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) QM_IDLE
1w6d: ISAKMP (0:2): purging node 1324880791
1w6d: ISAKMP: Sending phase 1 responder lifetime 86400

1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

1w6d: ISAKMP (0:2): Need XAUTH
1w6d: AAA: parse name=ISAKMP idb type=-1 tty=-1
1w6d: AAA/MEMORY: create_user (0x812F79FC) user='NULL'
   ruser='NULL' ds0=0 port='
ISAKMP' rem_addr='192.168.60.34' authen_type=ASCII service=LOGIN
   priv=0 initial_task_id='0'
1w6d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT

1w6d: AAA/AUTHEN/START (2017610393): port='ISAKMP' list='userauthen'
   action=LOGIN service=LOGIN
1w6d: AAA/AUTHEN/START (2017610393): found list userauthen
1w6d: AAA/AUTHEN/START (2017610393): Method=tacacs+ (tacacs+)
1w6d: TAC+: send AUTHEN/START packet ver=192 id=2017610393
1w6d: TAC+: Using default tacacs server-group "tacacs+" list.
1w6d: TAC+: Opening TCP/IP to 172.16.124.96/49 timeout=5
1w6d: TAC+: Opened TCP/IP handle 0x8183D638 to 172.16.124.96/49
1w6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/START/LOGIN/ASCII queued
1w6d: TAC+: (2017610393) AUTHEN/START/LOGIN/ASCII processed
1w6d: TAC+: ver=192 id=2017610393 received AUTHEN status = GETUSER
1w6d: AAA/AUTHEN(2017610393): Status=GETUSER
1w6d: ISAKMP: got callback 1
1w6d: ISAKMP/xauth: request attribute XAUTH_TYPE_V2
1w6d: ISAKMP/xauth: request attribute XAUTH_MESSAGE_V2
1w6d: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
1w6d: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): initiating peer config to 192.168.60.34. ID = 1641488057
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_XAUTH
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_START_LOGIN
Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
   New State = IKE_XAUTH_REQ_SENT

1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) CONF_XAUTH
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.
   message ID = 1641488057
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP: Config payload REPLY
1w6d: ISAKMP/xauth: reply attribute XAUTH_TYPE_V2 unexpected
1w6d: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
1w6d: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
1w6d: ISAKMP (0:2): deleting node 1641488057 error FALSE
   reason "done with xauth request/reply exchange"
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY
Old State = IKE_XAUTH_REQ_SENT
   New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

1w6d: AAA/AUTHEN/CONT (2017610393): continue_login (user='(undef)')
1w6d: AAA/AUTHEN(2017610393): Status=GETUSER
1w6d: AAA/AUTHEN(2017610393): Method=tacacs+ (tacacs+)
1w6d: TAC+: send AUTHEN/CONT packet id=2017610393
1w6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/CONT queued
1w6d: TAC+: (2017610393) AUTHEN/CONT processed
```

1w6d: TAC+: ver=192 id=2017610393 received AUTHEN status = GETPASS
1w6d: AAA/AUTHEN(2017610393): Status=GETPASS
1w6d: AAA/AUTHEN/CONT (2017610393): continue_login (user='cisco')
1w6d: AAA/AUTHEN(2017610393): Status=GETPASS
1w6d: AAA/AUTHEN(2017610393): Method=tacacs+ (tacacs+)
1w6d: TAC+: send AUTHEN/CONT packet id=2017610393
1w6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/CONT queued
1w6d: TAC+: (2017610393) AUTHEN/CONT processed
1w6d: TAC+: ver=192 id=2017610393 received AUTHEN status = PASS
1w6d: AAA/AUTHEN(2017610393): Status=PASS
1w6d: ISAKMP: got callback 1
1w6d: TAC+: Closing TCP/IP 0x8183D638 connection to 172.16.124.96/49
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): initiating peer config to 192.168.60.34. ID = 1736579999
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_XAUTH
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_CONT_LOGIN
Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
   New State = IKE_XAUTH_SET_SENT

1w6d: AAA/MEMORY: free_user (0x812F79FC) user='cisco' ruser='NULL'
   port='ISAKMP' rem_addr='192.168.60.34' authen_type=ASCII
   service=LOGIN priv=0
1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) CONF_XAUTH
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.
   message ID = 1736579999
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP: Config payload ACK
1w6d: ISAKMP (0:2): XAUTH ACK Processed
1w6d: ISAKMP (0:2): deleting node 1736579999 error FALSE
   reason "done with transaction"
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK
Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE

1w6d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.
   message ID = 398811763
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP: Config payload REQUEST
1w6d: ISAKMP (0:2): checking request:
1w6d: ISAKMP: IP4_ADDRESS
1w6d: ISAKMP: IP4_NETMASK
1w6d: ISAKMP: IP4_DNS
1w6d: ISAKMP: IP4_NBNS
1w6d: ISAKMP: ADDRESS_EXPIRY
1w6d: ISAKMP: APPLICATION_VERSION
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7000
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7001
1w6d: ISAKMP: DEFAULT_DOMAIN
1w6d: ISAKMP: SPLIT_INCLUDE
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7007
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7008
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7005
1w6d: AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1
1w6d: AAA/MEMORY: create_user (0x812F79FC) user='vpngroup' ruser='NULL' ds0=0 po
rt='ISAKMP-GROUP-AUTH' rem_addr='192.168.60.34' authen_type=NONE service=LOGIN pr

```
iv=0 initial_task_id='0'
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
   Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET
1w6d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(1059453615)
   user='vpngroup'
1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
   send AV service=ike
1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
   send AV protocol=ipsec
1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
   found list "groupauthor"
1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
   Method=LOCAL
1w6d: AAA/AUTHOR (1059453615): Post authorization status = PASS_ADD
1w6d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV service=ike
AAA/AUTHOR/IKE: Processing AV protocol=ipsec
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com
AAA/AUTHOR/IKE: Processing AV addr-pool*ippool
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV timeout*0
AAA/AUTHOR/IKE: Processing AV idletime*0
AAA/AUTHOR/IKE: Processing AV inacl*102
AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0
AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0
1w6d: ISAKMP (0:2): attributes sent in message:
1w6d: Address: 0.2.0.0
1w6d: ISAKMP (0:2): allocating address 10.1.1.114
1w6d: ISAKMP: Sending private address: 10.1.1.114
1w6d: ISAKMP: Unknown Attr: IP4_NETMASK (0x2)
1w6d: ISAKMP: Sending IP4_DNS server address: 10.1.1.10
1w6d: ISAKMP: Sending IP4_NBNS server address: 10.1.1.20
1w6d: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 86396
1w6d: ISAKMP: Sending APPLICATION_VERSION string:
   Cisco Internetwork Operating System Software IOS (tm) C1700 Software
   (C1710-K9O3SY-M), Version 12.2(8)T1, RELEASE SOFTWARE (fc2)
   TAC Support: http://www.cisco.com/tac
   Copyright (c) 1986-2002 by cisco Systems, Inc.
   Compiled Sat 30-Mar-02 13:30 by ccai
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7000)
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7001)
1w6d: ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com
1w6d: ISAKMP: Sending split include name 102 network 10.38.0.0
   mask 255.255.0.0 protocol 0, src port 0, dst port 0

1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7007)
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7008)
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7005)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): responding to peer config from 192.168.60.34. ID = 398811763
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_ADDR
1w6d: ISAKMP (0:2): deleting node 398811763 error FALSE reason ""
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

1w6d: AAA/MEMORY: free_user (0x812F79FC) user='vpngroup'
   ruser='NULL' port='ISAKMP-GROUP-AUTH' rem_addr='192.168.60.34'
   authen_type=NONE service=LOGIN priv=0
```

```
1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): processing HASH payload. message ID = 1369459046
1w6d: ISAKMP (0:2): processing SA payload. message ID = 1369459046
1w6d: ISAKMP (0:2): Checking IPSec proposal 1
1w6d: ISAKMP: transform 1, ESP_3DES
1w6d: ISAKMP: attributes in transform:
1w6d: ISAKMP: authenticator is HMAC-MD5
1w6d: ISAKMP: encaps is 1
1w6d: ISAKMP: SA life type in seconds
1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: validate proposal 0
1w6d: IPSEC(validate_proposal): transform proposal
   (prot 3, trans 3, hmac_alg 1) not supported
1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w6d: ISAKMP (0:2): skipping next ANDed proposal (1)
1w6d: ISAKMP (0:2): Checking IPSec proposal 2
1w6d: ISAKMP: transform 1, ESP_3DES
1w6d: ISAKMP: attributes in transform:
1w6d: ISAKMP: authenticator is HMAC-SHA
1w6d: ISAKMP: encaps is 1
1w6d: ISAKMP: SA life type in seconds
1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: validate proposal 0
1w6d: ISAKMP (0:2): atts are acceptable.
1w6d: ISAKMP (0:2): Checking IPSec proposal 2
1w6d: ISAKMP (0:2): transform 1, IPPCP LZS
1w6d: ISAKMP: attributes in transform:
1w6d: ISAKMP: encaps is 1
1w6d: ISAKMP: SA life type in seconds
1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: IPSEC(validate_proposal): transform proposal
   (prot 4, trans 3, hmac_alg 0) not supported
1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w6d: ISAKMP (0:2): Checking IPSec proposal 3
1w6d: ISAKMP: transform 1, ESP_3DES
1w6d: ISAKMP: attributes in transform:
1w6d: ISAKMP: authenticator is HMAC-MD5
1w6d: ISAKMP: encaps is 1
1w6d: ISAKMP: SA life type in seconds
1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: validate proposal 0
1w6d: IPSEC(validate_proposal): transform proposal
   (prot 3, trans 3, hmac_alg 1) not supported
1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w6d: ISAKMP (0:2): Checking IPSec proposal 4
1w6d: ISAKMP: transform 1, ESP_3DES
1w6d: ISAKMP: attributes in transform:
1w6d: ISAKMP: authenticator is HMAC-SHA
1w6d: ISAKMP: encaps is 1
1w6d: ISAKMP: SA life type in seconds
1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: validate proposal 0
1w6d: ISAKMP (0:2): atts are acceptable.
1w6d: IPSEC(validate_proposal_request): proposal part #1,
   (key eng. msg.) INBOUND local= 172.18.124.158,
   remote= 192.168.60.34, local_proxy= 172.18.124.158/255.255.255.255/0/0
   (type=1), remote_proxy= 10.1.1.114/255.255.255.255/0/0 (type=1),
   protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 0s and 0kb,
   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
1w6d: validate proposal request 0
1w6d: ISAKMP (0:2): processing NONCE payload. message ID = 1369459046
```

```
1w6d: ISAKMP (0:2): processing ID payload. message ID = 1369459046
1w6d: ISAKMP (0:2): processing ID payload. message ID = 1369459046
1w6d: ISAKMP (0:2): asking for 1 spis from ipsec
1w6d: ISAKMP (0:2): Node 1369459046, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE

1w6d: IPSEC(key_engine): got a queue event...
1w6d: IPSEC(spi_response): getting spi 1640315492 for SA
   from 172.18.124.158 to 192.168.60.34 for prot 3
1w6d: ISAKMP: received ke message (2/1)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) QM_IDLE
1w6d: ISAKMP (0:2): Node 1369459046,
   Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2

1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ipsec allocate flow 0
1w6d: ipsec allocate flow 0
1w6d: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)
1w6d: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)
1w6d: ISAKMP (0:2): Creating IPSec SAs
1w6d: inbound SA from 192.168.60.34 to 172.18.124.158
   (proxy 10.1.1.114 to 172.18.124.158)
1w6d: has spi 0x61C53A64 and conn_id 200 and flags 4
1w6d: lifetime of 2147483 seconds
1w6d: outbound SA from 172.18.124.158 to 192.168.60.34
   (proxy 172.18.124.158 to 10.1.1.114 )
1w6d: has spi -1885622177 and conn_id 201 and flags C
1w6d: lifetime of 2147483 seconds
1w6d: ISAKMP (0:2): deleting node 1369459046 error FALSE
   reason "quick mode done (await()"
1w6d: ISAKMP (0:2): Node 1369459046,
   Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

1w6d: IPSEC(key_engine): got a queue event...
1w6d: IPSEC(initialize_sas): ,
   (key eng. msg.) INBOUND local= 172.18.124.158,
   remote= 192.168.60.34, local_proxy= 172.18.124.158/0.0.0.0/0/0
   (type=1), remote_proxy= 10.1.1.114/0.0.0.0/0/0 (type=1),
   protocol= ESP, transform= esp-3des esp-sha-hmac ,
   lifedur= 2147483s and 0kb, spi= 0x61C53A64(1640315492),
   conn_id= 200, keysize= 0, flags= 0x4
1w6d: IPSEC(initialize_sas): , (key eng. msg.)
   OUTBOUND local= 172.18.124.158, remote= 192.168.60.34,
   local_proxy= 172.18.124.158/0.0.0.0/0/0 (type=1),
   remote_proxy= 10.1.1.114/0.0.0.0/0/0 (type=1),
   protocol= ESP, transform= esp-3des esp-sha-hmac ,
   lifedur= 2147483s and 0kb, spi= 0x8F9BB05F(2409345119),
   conn_id= 201, keysize= 0, flags= 0xC
1w6d: IPSEC(create_sa): sa created, (sa) sa_dest= 172.18.124.158,
   sa_prot= 50, sa_spi= 0x61C53A64(1640315492),
   sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 200
1w6d: IPSEC(create_sa): sa created, (sa) sa_dest= 192.168.60.34,
   sa_prot= 50, sa_spi= 0x8F9BB05F(2409345119),
   sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 201
```

Logs de client

Afin de visualiser les logs, lancer le visualiseur de log sur le client vpn, et placer le filtre à la *haute* pour toutes les classes configurées.

La sortie de log témoin est affichée ici.

```
1710#show debug
General OS:
TACACS access control debugging is on
AAA Authentication debugging is on
AAA Authorization debugging is on
Cryptographic Subsystem:
Crypto ISAKMP debugging is on
Crypto Engine debugging is on
Crypto IPSEC debugging is on


1710#
1w6d: ISAKMP (0:0): received packet from 192.168.60.34 (N) NEW SA
1w6d: ISAKMP: local port 500, remote port 500
1w6d: ISAKMP (0:2): (Re)Setting client xauth list userauthen and state
1w6d: ISAKMP: Locking CONFIG struct 0x8158B894 from
   crypto_ikmp_config_initialize_sa, count 2
1w6d: ISAKMP (0:2): processing SA payload. message ID = 0
1w6d: ISAKMP (0:2): processing ID payload. message ID = 0
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): vendor ID seems Unity/DPD but bad major
1w6d: ISAKMP (0:2): vendor ID is XAUTH
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): vendor ID is DPD
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): vendor ID is Unity
1w6d: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 3 policy
1w6d: ISAKMP: encryption 3DES-CBC
1w6d: ISAKMP: hash SHA
1w6d: ISAKMP: default group 2
1w6d: ISAKMP: auth XAUTHInitPreShared
1w6d: ISAKMP: life type in seconds
1w6d: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: ISAKMP (0:2): atts are acceptable. Next payload is 3
1w6d: CryptoEngine0: generate alg parameter
1w6d: CryptoEngine0: CRYPTO_ISA_DH_CREATE(hw)(ipsec)
1w6d: CRYPTO_ENGINE: Dh phase 1 status: 0
1w6d: ISAKMP (0:2): processing KE payload. message ID = 0
1w6d: CryptoEngine0: generate alg parameter
1w6d: CryptoEngine0: CRYPTO_ISA_DH_SHARE_SECRET(hw)(ipsec)
1w6d: ISAKMP (0:2): processing NONCE payload. message ID = 0
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1
1w6d: AAA/MEMORY: create_user (0x817F63F4) user='vpngroup' ruser='NULL' ds0=0
   port='ISAKMP-ID-AUTH' rem_addr='192.168.60.34' authen_type=NONE
   service=LOGIN priv=0 initial_task_id='0'
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT

1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894):
   Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET
1w6d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(1472763894) user='vpngroup'
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): send AV service=ike
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): send AV protocol=ipsec
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): found list "groupauthor"
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): Method=LOCAL
```

```
1w6d: AAA/AUTHOR (1472763894): Post authorization status = PASS_ADD
1w6d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV service=ike
AAA/AUTHOR/IKE: Processing AV protocol=ipsec
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com
AAA/AUTHOR/IKE: Processing AV addr-pool*ippool
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV timeout*0
AAA/AUTHOR/IKE: Processing AV idletime*0
AAA/AUTHOR/IKE: Processing AV inacl*102
AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0
AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0
1w6d: CryptoEngine0: create ISAKMP SKEYID for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_SA_CREATE(hw)(ipsec)
1w6d: ISAKMP (0:2): SKEYID state generated
1w6d: ISAKMP (0:2): SA is doing pre-shared key authentication plux
   XAUTH using id type ID_IPV4_ADDR
1w6d: ISAKMP (2): ID payload
next-payload : 10
type : 1
protocol : 17
port : 500
length : 8
1w6d: ISAKMP (2): Total payload length: 12
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) AG_INIT_EXCH
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

1w6d: AAA/MEMORY: free_user (0x817F63F4) user='vpngroup'
   ruser='NULL' port='ISAK MP-ID-AUTH' rem_addr='192.168.60.34'
   authen_type=NONE service=LOGIN priv=0
1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) AG_INIT_EXCH
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): processing HASH payload. message ID = 0
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): processing NOTIFY INITIAL_CONTACT protocol 1
   spi 0, message ID = 0, sa = 81673884
1w6d: ISAKMP (0:2): Process initial contact, bring down
   existing phase 1 and 2 SA's
1w6d: ISAKMP (0:2): returning IP addr to the address pool: 10.1.1.113
1w6d: ISAKMP (0:2): returning address 10.1.1.113 to pool
1w6d: ISAKMP (0:2): peer does not do paranoid keepalives.

1w6d: ISAKMP (0:2): SA has been authenticated with 192.168.60.34
1w6d: CryptoEngine0: clear dh number for conn id 1
1w6d: CryptoEngine0: CRYPTO_ISA_DH_DELETE(hw)(ipsec)
1w6d: IPSEC(key_engine): got a queue event...
1w6d: IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
1w6d: IPSEC(key_engine_delete_sas): delete all SAs shared with 192.168.60.34
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) QM_IDLE
1w6d: ISAKMP (0:2): purging node 1324880791
1w6d: ISAKMP: Sending phase 1 responder lifetime 86400

1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

1w6d: ISAKMP (0:2): Need XAUTH
```

```
1w6d: AAA: parse name=ISAKMP idb type=-1 tty=-1
1w6d: AAA/MEMORY: create_user (0x812F79FC) user='NULL'
   ruser='NULL' ds0=0 port='
ISAKMP' rem_addr='192.168.60.34' authen_type=ASCII service=LOGIN
   priv=0 initial_task_id='0'
1w6d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT

1w6d: AAA/AUTHEN/START (2017610393): port='ISAKMP' list='userauthen'
   action=LOGIN service=LOGIN
1w6d: AAA/AUTHEN/START (2017610393): found list userauthen
1w6d: AAA/AUTHEN/START (2017610393): Method=tacacs+ (tacacs+)
1w6d: TAC+: send AUTHEN/START packet ver=192 id=2017610393
1w6d: TAC+: Using default tacacs server-group "tacacs+" list.
1w6d: TAC+: Opening TCP/IP to 172.16.124.96/49 timeout=5
1w6d: TAC+: Opened TCP/IP handle 0x8183D638 to 172.16.124.96/49
1w6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/START/LOGIN/ASCII queued
1w6d: TAC+: (2017610393) AUTHEN/START/LOGIN/ASCII processed
1w6d: TAC+: ver=192 id=2017610393 received AUTHEN status = GETUSER
1w6d: AAA/AUTHEN(2017610393): Status=GETUSER
1w6d: ISAKMP: got callback 1
1w6d: ISAKMP/xauth: request attribute XAUTH_TYPE_V2
1w6d: ISAKMP/xauth: request attribute XAUTH_MESSAGE_V2
1w6d: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
1w6d: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): initiating peer config to 192.168.60.34. ID = 1641488057
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_XAUTH
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_START_LOGIN
Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
   New State = IKE_XAUTH_REQ_SENT

1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) CONF_XAUTH
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.
   message ID = 1641488057
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP: Config payload REPLY
1w6d: ISAKMP/xauth: reply attribute XAUTH_TYPE_V2 unexpected
1w6d: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
1w6d: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
1w6d: ISAKMP (0:2): deleting node 1641488057 error FALSE
   reason "done with xauth request/reply exchange"
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY
Old State = IKE_XAUTH_REQ_SENT
   New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

1w6d: AAA/AUTHEN/CONT (2017610393): continue_login (user='(undef)')
1w6d: AAA/AUTHEN(2017610393): Status=GETUSER
1w6d: AAA/AUTHEN(2017610393): Method=tacacs+ (tacacs+)
1w6d: TAC+: send AUTHEN/CONT packet id=2017610393
1w6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/CONT queued
1w6d: TAC+: (2017610393) AUTHEN/CONT processed
1w6d: TAC+: ver=192 id=2017610393 received AUTHEN status = GETPASS
1w6d: AAA/AUTHEN(2017610393): Status=GETPASS
1w6d: AAA/AUTHEN/CONT (2017610393): continue_login (user='cisco')
1w6d: AAA/AUTHEN(2017610393): Status=GETPASS
1w6d: AAA/AUTHEN(2017610393): Method=tacacs+ (tacacs+)
1w6d: TAC+: send AUTHEN/CONT packet id=2017610393
1w6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/CONT queued
1w6d: TAC+: (2017610393) AUTHEN/CONT processed
```

```
1w6d: TAC+: ver=192 id=2017610393 received AUTHEN status = PASS
1w6d: AAA/AUTHEN(2017610393): Status=PASS
1w6d: ISAKMP: got callback 1
1w6d: TAC+: Closing TCP/IP 0x8183D638 connection to 172.16.124.96/49
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): initiating peer config to 192.168.60.34. ID = 1736579999
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_XAUTH
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_CONT_LOGIN
Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
   New State = IKE_XAUTH_SET_SENT

1w6d: AAA/MEMORY: free_user (0x812F79FC) user='cisco' ruser='NULL'
   port='ISAKMP' rem_addr='192.168.60.34' authen_type=ASCII
   service=LOGIN priv=0
1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) CONF_XAUTH
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.
   message ID = 1736579999
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP: Config payload ACK
1w6d: ISAKMP (0:2): XAUTH ACK Processed
1w6d: ISAKMP (0:2): deleting node 1736579999 error FALSE
   reason "done with transaction"
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK
Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE

1w6d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.
   message ID = 398811763
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP: Config payload REQUEST
1w6d: ISAKMP (0:2): checking request:
1w6d: ISAKMP: IP4_ADDRESS
1w6d: ISAKMP: IP4_NETMASK
1w6d: ISAKMP: IP4_DNS
1w6d: ISAKMP: IP4_NBNS
1w6d: ISAKMP: ADDRESS_EXPIRY
1w6d: ISAKMP: APPLICATION_VERSION
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7000
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7001
1w6d: ISAKMP: DEFAULT_DOMAIN
1w6d: ISAKMP: SPLIT_INCLUDE
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7007
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7008
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7005
1w6d: AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1
1w6d: AAA/MEMORY: create_user (0x812F79FC) user='vpngroup' ruser='NULL' ds0=0 po
rt='ISAKMP-GROUP-AUTH' rem_addr='192.168.60.34' authen_type=NONE service=LOGIN pr
iv=0 initial_task_id='0'
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
   Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET
1w6d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(1059453615)
   user='vpngroup'
```

```
1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
   send AV service=ike
1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
   send AV protocol=ipsec
1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
   found list "groupauthor"
1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
   Method=LOCAL
1w6d: AAA/AUTHOR (1059453615): Post authorization status = PASS_ADD
1w6d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV service=ike
AAA/AUTHOR/IKE: Processing AV protocol=ipsec
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com
AAA/AUTHOR/IKE: Processing AV addr-pool*ippool
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV timeout*0
AAA/AUTHOR/IKE: Processing AV idletime*0
AAA/AUTHOR/IKE: Processing AV inacl*102
AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0
AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0
1w6d: ISAKMP (0:2): attributes sent in message:
1w6d: Address: 0.2.0.0
1w6d: ISAKMP (0:2): allocating address 10.1.1.114
1w6d: ISAKMP: Sending private address: 10.1.1.114
1w6d: ISAKMP: Unknown Attr: IP4_NETMASK (0x2)
1w6d: ISAKMP: Sending IP4_DNS server address: 10.1.1.10
1w6d: ISAKMP: Sending IP4_NBNS server address: 10.1.1.20
1w6d: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 86396
1w6d: ISAKMP: Sending APPLICATION_VERSION string:
   Cisco Internetwork Operating System Software IOS (tm) C1700 Software
   (C1710-K9O3SY-M), Version 12.2(8)T1, RELEASE SOFTWARE (fc2)
   TAC Support: http://www.cisco.com/tac
   Copyright (c) 1986-2002 by cisco Systems, Inc.
   Compiled Sat 30-Mar-02 13:30 by ccai
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7000)
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7001)
1w6d: ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com
1w6d: ISAKMP: Sending split include name 102 network 10.38.0.0
   mask 255.255.0.0 protocol 0, src port 0, dst port 0

1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7007)
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7008)
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7005)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): responding to peer config from 192.168.60.34. ID = 398811763
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_ADDR
1w6d: ISAKMP (0:2): deleting node 398811763 error FALSE reason ""
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

1w6d: AAA/MEMORY: free_user (0x812F79FC) user='vpngroup'
   ruser='NULL' port='ISAKMP-GROUP-AUTH' rem_addr='192.168.60.34'
   authen_type=NONE service=LOGIN priv=0
1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): processing HASH payload. message ID = 1369459046
1w6d: ISAKMP (0:2): processing SA payload. message ID = 1369459046
1w6d: ISAKMP (0:2): Checking IPSec proposal 1
1w6d: ISAKMP: transform 1, ESP_3DES
```

```
1w6d: ISAKMP: attributes in transform:
1w6d: ISAKMP: authenticator is HMAC-MD5
1w6d: ISAKMP: encaps is 1
1w6d: ISAKMP: SA life type in seconds
1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: validate proposal 0
1w6d: IPSEC(validate_proposal): transform proposal
   (prot 3, trans 3, hmac_alg 1) not supported
1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w6d: ISAKMP (0:2): skipping next ANDed proposal (1)
1w6d: ISAKMP (0:2): Checking IPSec proposal 2
1w6d: ISAKMP: transform 1, ESP_3DES
1w6d: ISAKMP: attributes in transform:
1w6d: ISAKMP: authenticator is HMAC-SHA
1w6d: ISAKMP: encaps is 1
1w6d: ISAKMP: SA life type in seconds
1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: validate proposal 0
1w6d: ISAKMP (0:2): atts are acceptable.
1w6d: ISAKMP (0:2): Checking IPSec proposal 2
1w6d: ISAKMP (0:2): transform 1, IPPCP LZS
1w6d: ISAKMP: attributes in transform:
1w6d: ISAKMP: encaps is 1
1w6d: ISAKMP: SA life type in seconds
1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: IPSEC(validate_proposal): transform proposal
   (prot 4, trans 3, hmac_alg 0) not supported
1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w6d: ISAKMP (0:2): Checking IPSec proposal 3
1w6d: ISAKMP: transform 1, ESP_3DES
1w6d: ISAKMP: attributes in transform:
1w6d: ISAKMP: authenticator is HMAC-MD5
1w6d: ISAKMP: encaps is 1
1w6d: ISAKMP: SA life type in seconds
1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: validate proposal 0
1w6d: IPSEC(validate_proposal): transform proposal
   (prot 3, trans 3, hmac_alg 1) not supported
1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w6d: ISAKMP (0:2): Checking IPSec proposal 4
1w6d: ISAKMP: transform 1, ESP_3DES
1w6d: ISAKMP: attributes in transform:
1w6d: ISAKMP: authenticator is HMAC-SHA
1w6d: ISAKMP: encaps is 1
1w6d: ISAKMP: SA life type in seconds
1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: validate proposal 0
1w6d: ISAKMP (0:2): atts are acceptable.
1w6d: IPSEC(validate_proposal_request): proposal part #1,
   (key eng. msg.) INBOUND local= 172.18.124.158,
   remote= 192.168.60.34, local_proxy= 172.18.124.158/255.255.255.255/0/0
   (type=1), remote_proxy= 10.1.1.114/255.255.255.255/0/0 (type=1),
   protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 0s and 0kb,
   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
1w6d: validate proposal request 0
1w6d: ISAKMP (0:2): processing NONCE payload. message ID = 1369459046
1w6d: ISAKMP (0:2): processing ID payload. message ID = 1369459046
1w6d: ISAKMP (0:2): processing ID payload. message ID = 1369459046
1w6d: ISAKMP (0:2): asking for 1 spis from ipsec
1w6d: ISAKMP (0:2): Node 1369459046, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE

1w6d: IPSEC(key_engine): got a queue event...
1w6d: IPSEC(spi_response): getting spi 1640315492 for SA
```

```
   from 172.18.124.158 to 192.168.60.34 for prot 3
1w6d: ISAKMP: received ke message (2/1)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) QM_IDLE
1w6d: ISAKMP (0:2): Node 1369459046,
   Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2

1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ipsec allocate flow 0
1w6d: ipsec allocate flow 0
1w6d: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)
1w6d: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)
1w6d: ISAKMP (0:2): Creating IPSec SAs
1w6d: inbound SA from 192.168.60.34 to 172.18.124.158
   (proxy 10.1.1.114 to 172.18.124.158)
1w6d: has spi 0x61C53A64 and conn_id 200 and flags 4
1w6d: lifetime of 2147483 seconds
1w6d: outbound SA from 172.18.124.158 to 192.168.60.34
   (proxy 172.18.124.158 to 10.1.1.114 )
1w6d: has spi -1885622177 and conn_id 201 and flags C
1w6d: lifetime of 2147483 seconds
1w6d: ISAKMP (0:2): deleting node 1369459046 error FALSE
   reason "quick mode done (await()"
1w6d: ISAKMP (0:2): Node 1369459046,
   Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

1w6d: IPSEC(key_engine): got a queue event...
1w6d: IPSEC(initialize_sas): ,
   (key eng. msg.) INBOUND local= 172.18.124.158,
   remote= 192.168.60.34, local_proxy= 172.18.124.158/0.0.0.0/0/0
   (type=1), remote_proxy= 10.1.1.114/0.0.0.0/0/0 (type=1),
   protocol= ESP, transform= esp-3des esp-sha-hmac ,
   lifedur= 2147483s and 0kb, spi= 0x61C53A64(1640315492),
   conn_id= 200, keysize= 0, flags= 0x4
1w6d: IPSEC(initialize_sas): , (key eng. msg.)
   OUTBOUND local= 172.18.124.158, remote= 192.168.60.34,
   local_proxy= 172.18.124.158/0.0.0.0/0/0 (type=1),
   remote_proxy= 10.1.1.114/0.0.0.0/0/0 (type=1),
   protocol= ESP, transform= esp-3des esp-sha-hmac ,
   lifedur= 2147483s and 0kb, spi= 0x8F9BB05F(2409345119),
   conn_id= 201, keysize= 0, flags= 0xC
1w6d: IPSEC(create_sa): sa created, (sa) sa_dest= 172.18.124.158,
   sa_prot= 50, sa_spi= 0x61C53A64(1640315492),
   sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 200
1w6d: IPSEC(create_sa): sa created, (sa) sa_dest= 192.168.60.34,
   sa_prot= 50, sa_spi= 0x8F9BB05F(2409345119),
   sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 201
```

Informations connexes

- Support de Terminal Access Controller Access Control System (TACACS+)
- Support de Cisco Secure Access Control Server pour Unix
- Cisco Secure ACS pour le support de Windows
- Support de Client VPN Cisco

- Support de Négociation IPSec/protocoles IKE
- Support et documentation techniques - Cisco Systems