

# Configuration d'IPSec sur TCP sur un concentrateur Cisco VPN 3000 avec VPN Client version 3.5 et ultérieure

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez le concentrateur VPN 3000](#)

[Instructions pas à pas](#)

[Configurer le client VPN](#)

[Vérifiez les connexions sur le concentrateur VPN 3000](#)

[Dépannez](#)

[Dépannage des commandes](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment configurer la sécurité IP (IPSec) au-dessus du Protocole TCP (Transmission Control Protocol). Ceci permet à un client vpn de fonctionner dans un environnement dans lequel Encapsulating Security Protocol standard (ESP, Protocole 50) ou échange de clés Internet (IKE) (IKE, Protocole UDP (User Datagram Protocol) 500) ne peut pas fonctionner, ou peut fonctionner seulement avec la modification aux règles existantes de Pare-feu. IPSec au-dessus de TCP encapsule l'IKE et des protocoles IPsecs dans un paquet TCP, et il active le Tunnellisation sécurisé par les deux Traduction d'adresses de réseau (NAT) et périphériques et Pare-feu de translation d'adresses d'adresse du port (PAT).

**Remarque:** IPSec au-dessus de TCP ne fonctionne pas avec des Pare-feu basés sur proxy.

IPSec au-dessus de TCP fonctionne avec le client de logiciel VPN et le client matériel VPN 3002. C'est un client à la caractéristique de concentrateur seulement. Cela ne fonctionne pas pour des connexions entre réseaux locaux.

Le concentrateur VPN 3000 peut simultanément prendre en charge IPSec standard, IPSec au-dessus de TCP, et IPSec au-dessus de l'UDP, basé sur le client avec lequel il des données d'échanges.

Le client matériel VPN 3002, qui prend en charge un tunnel à la fois, peut se connecter utilisant IPSec standard, IPSec au-dessus de TCP, ou IPSec au-dessus d'UDP.

# Conditions préalables

## Conditions requises

L'interface publique du concentrateur VPN 3000 devrait être configurée. IPSec au-dessus de TCP est pris en charge seulement sur l'interface publique sur les Ethernets 2. se rapportent au pour en savoir plus de [notes de mise à jour en Client VPN Cisco](#).

## Composants utilisés

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

- Version 3.5 ou ultérieures de concentrateur VPN 3000
- Version du client 3.5 VPN ou plus tard

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 de documents, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

# Configurez le concentrateur VPN 3000

## Instructions pas à pas

Terminez-vous ces étapes pour configurer le concentrateur VPN 3000.

1. Allez au **Configuration > User Management > Groups > ajoutent le groupe** et créent un nom de groupe et un mot de passe sur le concentrateur VPN. Cliquez sur Add sur la fin.

The screenshot shows the 'Add' page for creating a new group in the Cisco VPN 3000 configuration. The breadcrumb navigation is 'Configuration | User Management | Groups | Add'. A text box explains: 'This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.' Below this is a tabbed interface with 'Identity' selected. The 'Identity Parameters' table is as follows:

Attribute	Value	Description
Group Name	rtppvpn	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.

At the bottom of the form are 'Add' and 'Cancel' buttons.

2. Si le même groupe est utilisé par des utilisateurs sur des versions de client vpn plus tôt que

3.5, ou si vous utilisez IPSec au-dessus d'UDP sur le client vpn, alors sélectionnez **IPSec au-dessus d'UDP** sous l'onglet de config de client.

Client Configuration Parameters			
Cisco Client Parameters			
Attribute	Value	Inherit?	Description
Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPSec client to store the password locally.
IP Sec over UDP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IP Sec over UDP Port	10000	<input checked="" type="checkbox"/>	Enter the UDP port to be used for IPSec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IP Sec Backup Servers	Use Client Configured List <div style="border: 1px solid black; height: 100px;"></div>	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> <li>Select a method to use or disable backup servers.</li> <li>Enter up to 10 IPSec backup server addresses/names starting from high priority to low.</li> <li>Enter each IPSec backup server address/name on a single line.</li> </ul>
Microsoft Client Parameters			
Intercept DHCP Configure Message	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to use group policy for clients requesting Microsoft DHCP options
Subnet Mask	255.255.255.255	<input checked="" type="checkbox"/>	Enter the subnet mask for clients requesting Microsoft DHCP options.

- Allez au **Configuration > User Management > aux utilisateurs > modifiez l'esupport**. Si vous utilisez l'authentification interne, créez un utilisateur pour authentifier au groupe. Affectez alors l'utilisateur à ce groupe.

Configuration | User Management | Users | Modify esupport

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity Parameters		
Attribute	Value	Description
User Name	esupport	Enter a unique user name.
Password	*****	Enter the user's password. The password must satisfy the group password requirements.
Verify	*****	Verify the user's password.
Group	rtvpn	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Apply Cancel

- Allez à la **configuration > au Tunnellisation et à la Sécurité > transparence NAT** et sélectionnez **l'IPsec au-dessus de** l'option de TCP. Entrez dans jusqu'à 10 ports, utilisant une virgule pour séparer les ports. Vous n'avez pas besoin d'utiliser les espaces. Le port par défaut est 10,000. La plage est de 1 à 65,635. Si vous entrez dans un port connu (tel que port 80 (HTTP) ou port 443 (HTTPS)), le système affiche un avertissement que le protocole associé avec ce port ne travaille plus à l'interface publique. La conséquence est que vous ne pouvez plus utiliser un navigateur pour gérer le concentrateur VPN 3000 par l'interface publique. Pour résoudre ce problème, modifiez la Gestion HTTP/HTTPS à différents ports. Vous devez configurer le port TCP sur le client vpn aussi bien que sur le concentrateur VPN. La configuration de client doit inclure au moins un des ports que vous placez pour le

concentrateur VPN

ici.

Configuration | System | Tunneling Protocols | IPSec | IPSec over TCP

This section lets you configure system-wide IPSec over TCP operation.

**Enabled**

TCP Port(s)  Enter up to 10 comma-separated TCP ports (1 - 65535).

## [Configurer le client VPN](#)

Terminez-vous ces étapes pour configurer le client vpn.

1. Allez aux **options** > au **Properties**. Sous l'onglet Général, le **Tunnellisation transparent d'enable de contrôle** et choisissent l'**utilisation IPSec au-dessus du TCP**

Properties for 05-RTP

General | Authentication | Connections

Enter a description of this connection entry (optional):

Enable transparent tunneling

Allow IPSec over UDP (NAT/PAT)

Use IPSec over TCP (NAT/PAT/Firewall)

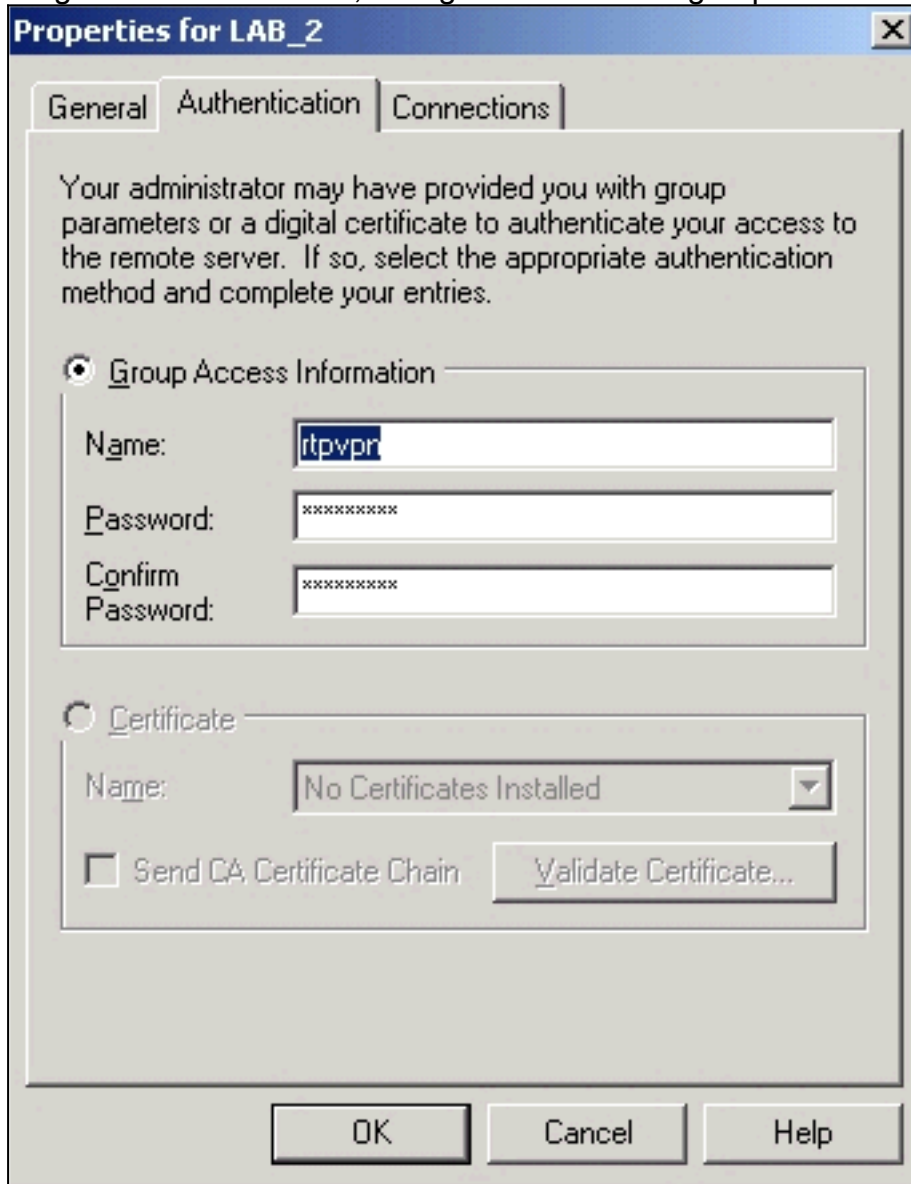
TCP port:

Allow local LAN access

Peer response timeout:  (30 - 480 seconds)

(NAT/PAT/Firewall).

2. Sous l'onglet d'authentification, configurez un nom de groupe et un mot de passe sur le



client.

## [Vérifiez les connexions sur le concentrateur VPN 3000](#)

La région de **Monitoring > Sessions** sur le concentrateur VPN 3000 vérifie la connexion des utilisateurs avec le même groupe pour IPSec au-dessus de TCP et IPSec au-dessus d'UDP.

Monitoring | Sessions Wednesday, 05 December 2001 10:39:01  
Reset Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group

### Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
0	2	1	3	3	20	26

LAN-to-LAN Sessions [ Remote Access Sessions | Management Sessions ]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
No LAN-to-LAN Sessions							

Remote Access Sessions [ LAN-to-LAN Sessions | Management Sessions ]

Username	Group	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
esupport	rtpvpn	64.102.55.209	172.18.124.217	IPSec/UDP	3DES-168	Dec 05 10:38:06	0:00:58	22416	1536
esupporttcp	rtpvpn	172.18.124.241	172.18.124.218	IPSec/TCP	3DES-168	Dec 05 10:39:02	0:00:02	64	72

## Dépannez

Cette section fournit des informations que vous pouvez utiliser pour 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:** Avant d'exécuter les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

L'enable met au point pour **AUTHENTIQUE**, **AUTHDBG**, **AUTHDECODE**, **IKE**, **IKEDBG**, **IKEDECODE**, **IPSEC**, **IPSECDBG**, **IPSECDECODE** pour les niveaux 1 à 13 sous la configuration **> le système > les événements > les classes**.

```
1203 12/05/2001 11:40:54.220 SEV=9 IKEDBG/0 RPT=5347 172.18.124.241
Group [rtpvpn] User [esupporttcp]
processing SA payload
```

```
1204 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5035 172.18.124.241
SA Payload Decode :
DOI : IPSEC (1)
Situation : Identity Only (1)
Length : 696
```

```
1207 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5036 172.18.124.241
Proposal Decode:
Proposal # : 1
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 98 79 D2 38
Length : 40
```

```
1211 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5037 172.18.124.241
```

Transform # 1 Decode for Proposal # 1:

Transform # : 1

Transform ID : Triple-DES (3)

Length : 28

1213 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5038 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: MD5 (1)

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1216 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5039 172.18.124.241

Proposal Decode:

Proposal # : 1

Protocol ID : IPCOMP (4)

#of Transforms: 1

Spi : 5D 82

Length : 34

1220 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5040 172.18.124.241

Transform # 1 Decode for Proposal # 1:

Transform # : 1

Transform ID : LZS (3)

Length : 24

1222 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5041 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1224 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5042 172.18.124.241

Proposal Decode:

Proposal # : 2

Protocol ID : ESP (3)

#of Transforms: 1

Spi : 98 79 D2 38

Length : 40

1228 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5043 172.18.124.241

Transform # 1 Decode for Proposal # 2:

Transform # : 1

Transform ID : Triple-DES (3)

Length : 28

1230 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5044 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: SHA (2)

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1233 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5045 172.18.124.241

Proposal Decode:

Proposal # : 2

Protocol ID : IPCOMP (4)

#of Transforms: 1

Spi : D8 44

Length : 34

1237 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5046 172.18.124.241

Transform # 1 Decode for Proposal # 2:

Transform # : 1

Transform ID : LZS (3)

Length : 24

1239 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5047 172.18.124.241  
Phase 2 SA Attribute Decode for Transform # 1:  
Encapsulation : Tunnel (1)  
Life Time : 2147483 seconds

1241 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5048 172.18.124.241  
Proposal Decode:  
Proposal # : 3  
Protocol ID : ESP (3)  
#of Transforms: 1  
Spi : 98 79 D2 38  
Length : 40

1245 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5049 172.18.124.241  
Transform # 1 Decode for Proposal # 3:  
Transform # : 1  
Transform ID : Triple-DES (3)  
Length : 28

1247 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5050 172.18.124.241  
Phase 2 SA Attribute Decode for Transform # 1:  
HMAC Algorithm: MD5 (1)  
Encapsulation : Tunnel (1)  
Life Time : 2147483 seconds

1250 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5051 172.18.124.241  
Proposal Decode:  
Proposal # : 4  
Protocol ID : ESP (3)  
#of Transforms: 1  
Spi : 98 79 D2 38  
Length : 40

1254 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5052 172.18.124.241  
Transform # 1 Decode for Proposal # 4:  
Transform # : 1  
Transform ID : Triple-DES (3)  
Length : 28

1256 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5053 172.18.124.241  
Phase 2 SA Attribute Decode for Transform # 1:  
HMAC Algorithm: SHA (2)  
Encapsulation : Tunnel (1)  
Life Time : 2147483 seconds

1259 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5054 172.18.124.241  
Proposal Decode:  
Proposal # : 5  
Protocol ID : ESP (3)  
#of Transforms: 1  
Spi : 98 79 D2 38  
Length : 40

1263 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5055 172.18.124.241  
Transform # 1 Decode for Proposal # 5:  
Transform # : 1  
Transform ID : DES-CBC (2)  
Length : 28

1265 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5056 172.18.124.241  
Phase 2 SA Attribute Decode for Transform # 1:  
HMAC Algorithm: MD5 (1)  
Encapsulation : Tunnel (1)  
Life Time : 2147483 seconds



1268 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5057 172.18.124.241

Proposal Decode:

Proposal # : 5

Protocol ID : IPCOMP (4)

#of Transforms: 1

Spi : 80 07

Length : 34

1272 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5058 172.18.124.241

Transform # 1 Decode for Proposal # 5:

Transform # : 1

Transform ID : LZS (3)

Length : 24

1274 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5059 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1276 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5060 172.18.124.241

Proposal Decode:

Proposal # : 6

Protocol ID : ESP (3)

#of Transforms: 1

Spi : 98 79 D2 38

Length : 40

1280 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5061 172.18.124.241

Transform # 1 Decode for Proposal # 6:

Transform # : 1

Transform ID : DES-CBC (2)

Length : 28

1282 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5062 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: SHA (2)

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1285 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5063 172.18.124.241

Proposal Decode:

Proposal # : 6

Protocol ID : IPCOMP (4)

#of Transforms: 1

Spi : 1A D4

Length : 34

1289 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5064 172.18.124.241

Transform # 1 Decode for Proposal # 6:

Transform # : 1

Transform ID : LZS (3)

Length : 24

1291 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5065 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1293 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5066 172.18.124.241

Proposal Decode:

Proposal # : 7

Protocol ID : ESP (3)

#of Transforms: 1

Spi : 98 79 D2 38  
Length : 40

1297 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5067 172.18.124.241  
Transform # 1 Decode for Proposal # 7:  
Transform # : 1  
Transform ID : DES-CBC (2)  
Length : 28

1299 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5068 172.18.124.241  
Phase 2 SA Attribute Decode for Transform # 1:  
HMAC Algorithm: MD5 (1)  
Encapsulation : Tunnel (1)  
Life Time : 2147483 seconds

1302 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5069 172.18.124.241  
Proposal Decode:  
Proposal # : 8  
Protocol ID : ESP (3)  
#of Transforms: 1  
Spi : 98 79 D2 38  
Length : 40

1306 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5070 172.18.124.241  
Transform # 1 Decode for Proposal # 8:  
Transform # : 1  
Transform ID : DES-CBC (2)  
Length : 28

1308 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5071 172.18.124.241  
Phase 2 SA Attribute Decode for Transform # 1:  
HMAC Algorithm: SHA (2)  
Encapsulation : Tunnel (1)  
Life Time : 2147483 seconds

1311 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5072 172.18.124.241  
Proposal Decode:  
Proposal # : 9  
Protocol ID : ESP (3)  
#of Transforms: 1  
Spi : 98 79 D2 38  
Length : 40

1315 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5073 172.18.124.241  
Transform # 1 Decode for Proposal # 9:  
Transform # : 1  
Transform ID : NULL (11)  
Length : 28

1317 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5074 172.18.124.241  
Phase 2 SA Attribute Decode for Transform # 1:  
HMAC Algorithm: MD5 (1)  
Encapsulation : Tunnel (1)  
Life Time : 2147483 seconds

1320 12/05/2001 11:40:54.220 SEV=8 IKEDECODE/0 RPT=5075 172.18.124.241  
Proposal Decode:  
Proposal # : 9  
Protocol ID : IPCOMP (4)  
#of Transforms: 1  
Spi : 7B 9B  
Length : 34

1324 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5076 172.18.124.241

Transform # 1 Decode for Proposal # 9:

Transform # : 1  
Transform ID : LZS (3)  
Length : 24

1326 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5077 172.18.124.241  
Phase 2 SA Attribute Decode for Transform # 1:  
Encapsulation : Tunnel (1)  
Life Time : 2147483 seconds

1328 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5078 172.18.124.241  
Proposal Decode:  
Proposal # : 10  
Protocol ID : ESP (3)  
#of Transforms: 1  
Spi : 98 79 D2 38  
Length : 40

1332 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5079 172.18.124.241  
Transform # 1 Decode for Proposal # 10:  
Transform # : 1  
Transform ID : NULL (11)  
Length : 28

1334 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5080 172.18.124.241  
Phase 2 SA Attribute Decode for Transform # 1:  
HMAC Algorithm: SHA (2)  
Encapsulation : Tunnel (1)  
Life Time : 2147483 seconds

1337 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5081 172.18.124.241  
Proposal Decode:  
Proposal # : 10  
Protocol ID : IPCOMP (4)  
#of Transforms: 1  
Spi : 79 45  
Length : 34

1341 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5082 172.18.124.241  
Transform # 1 Decode for Proposal # 10:  
Transform # : 1  
Transform ID : LZS (3)  
Length : 24

1343 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5083 172.18.124.241  
Phase 2 SA Attribute Decode for Transform # 1:  
Encapsulation : Tunnel (1)  
Life Time : 2147483 seconds

1345 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5084 172.18.124.241  
Proposal Decode:  
Proposal # : 11  
Protocol ID : ESP (3)  
#of Transforms: 1  
Spi : 98 79 D2 38  
Length : 40

1349 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5085 172.18.124.241  
Transform # 1 Decode for Proposal # 11:  
Transform # : 1  
Transform ID : NULL (11)  
Length : 28

1351 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5086 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: MD5 (1)

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1354 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5087 172.18.124.241

Proposal Decode:

Proposal # : 12

Protocol ID : ESP (3)

#of Transforms: 1

Spi : 98 79 D2 38

Length : 40

1358 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5088 172.18.124.241

Transform # 1 Decode for Proposal # 12:

Transform # : 1

Transform ID : NULL (11)

Length : 28

1360 12/05/2001 11:40:54.230 SEV=8 IKEDECODE/0 RPT=5089 172.18.124.241

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: SHA (2)

Encapsulation : Tunnel (1)

Life Time : 2147483 seconds

1363 12/05/2001 11:40:54.230 SEV=9 IKEDBG/1 RPT=666 172.18.124.241

Group [rtpvpn] User [esupporttcp]

processing nonce payload

1364 12/05/2001 11:40:54.230 SEV=9 IKEDBG/1 RPT=667 172.18.124.241

Group [rtpvpn] User [esupporttcp]

Processing ID

1365 12/05/2001 11:40:54.230 SEV=12 IKEDECODE/11 RPT=115

ID\_IPV4\_ADDR ID received

172.18.124.217

1366 12/05/2001 11:40:54.230 SEV=5 IKE/25 RPT=58 172.18.124.241

Group [rtpvpn] User [esupporttcp]

Received remote Proxy Host data in ID Payload:

Address 172.18.124.217, Protocol 0, Port 0

1369 12/05/2001 11:40:54.230 SEV=9 IKEDBG/1 RPT=668 172.18.124.241

Group [rtpvpn] User [esupporttcp]

Processing ID

1370 12/05/2001 11:40:54.230 SEV=12 IKEDECODE/11 RPT=116

ID\_IPV4\_ADDR\_SUBNET ID received

0.0.0.0

0.0.0.0

1371 12/05/2001 11:40:54.230 SEV=5 IKE/34 RPT=36 172.18.124.241

Group [rtpvpn] User [esupporttcp]

Received local IP Proxy Subnet data in ID Payload:

Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

1374 12/05/2001 11:40:54.230 SEV=5 IKE/66 RPT=58 172.18.124.241

Group [rtpvpn] User [esupporttcp]

IKE Remote Peer configured for SA: ESP-3DES-MD5

1376 12/05/2001 11:40:54.230 SEV=9 IKEDBG/0 RPT=5348 172.18.124.241

Group [rtpvpn] User [esupporttcp]

processing IPSEC SA

1377 12/05/2001 11:40:54.230 SEV=12 IKEDECODE/0 RPT=5090  
IKE Decode of received SA attributes follows:  
0000: 80050001 80040001 80010001 00020004 .....  
0010: 0020C49B . . .

1380 12/05/2001 11:40:54.230 SEV=12 IKEDECODE/0 RPT=5091  
IKE Decode of received SA attributes follows:  
0000: 80050002 80040001 80010001 00020004 .....  
0010: 0020C49B . . .

1383 12/05/2001 11:40:54.230 SEV=8 IKEDBG/0 RPT=5349  
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES  
Parsing received transform:  
Phase 2 failure:  
Mismatched attr types for class HMAC Algorithm:  
Rcv'd: SHA  
Cfg'd: MD5

1387 12/05/2001 11:40:54.230 SEV=12 IKEDECODE/0 RPT=5092  
IKE Decode of received SA attributes follows:  
0000: 80050001 80040001 80010001 00020004 .....  
0010: 0020C49B . . .

1390 12/05/2001 11:40:54.230 SEV=7 IKEDBG/27 RPT=58 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
IPSec SA Proposal # 3, Transform # 1 acceptable

1392 12/05/2001 11:40:54.230 SEV=7 IKEDBG/0 RPT=5350 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
IKE: requesting SPI!

1393 12/05/2001 11:40:54.230 SEV=9 IPSECDBG/6 RPT=282  
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000,  
seq 58, err 0, type 2, mode 0, state 32, label 0, pad 0,  
spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0,  
hmacAlg 0, lifetype 0, lifetime1 707832, lifetime2 0, dsId 300

1397 12/05/2001 11:40:54.230 SEV=9 IPSECDBG/1 RPT=1062  
Processing KEY\_GETSPI msg!

1398 12/05/2001 11:40:54.230 SEV=7 IPSECDBG/13 RPT=58  
Reserved SPI 1889854019

1399 12/05/2001 11:40:54.230 SEV=8 IKEDBG/6 RPT=58  
IKE got SPI from key engine: SPI = 0x70a4e243

1400 12/05/2001 11:40:54.230 SEV=9 IKEDBG/0 RPT=5351 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
oakley constructing quick mode

1401 12/05/2001 11:40:54.230 SEV=9 IKEDBG/0 RPT=5352 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
constructing blank hash

1402 12/05/2001 11:40:54.230 SEV=9 IKEDBG/0 RPT=5353 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
constructing ISA\_SA for ipsec

1403 12/05/2001 11:40:54.230 SEV=9 IKEDBG/1 RPT=669 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
constructing ipsec nonce payload

1404 12/05/2001 11:40:54.230 SEV=9 IKEDBG/1 RPT=670 172.18.124.241  
Group [rtpvpn] User [esupporttcp]

constructing proxy ID

1405 12/05/2001 11:40:54.230 SEV=7 IKEDBG/0 RPT=5354 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
Transmitting Proxy Id:  
Remote host: 172.18.124.217 Protocol 0 Port 0  
Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0

1409 12/05/2001 11:40:54.230 SEV=9 IKEDBG/0 RPT=5355 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
constructing qm hash

1410 12/05/2001 11:40:54.240 SEV=12 IKEDECODE/5 RPT=58  
IKE Responder sending 2nd QM pkt: msg id = f2a6ce35

1411 12/05/2001 11:40:54.240 SEV=8 IKEDBG/0 RPT=5356 172.18.124.241  
SENDING Message (msgid=f2a6ce35) with payloads :  
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)  
... total length : 152

1414 12/05/2001 11:40:54.250 SEV=8 IKEDECODE/0 RPT=5093 172.18.124.241  
ISAKMP HEADER : ( Version 1.0 )  
Initiator Cookie(8): E7 AC CD 06 A6 74 A7 1A  
Responder Cookie(8): 98 3B 37 97 CA 06 BC 18  
Next Payload : HASH (8)  
Exchange Type : Oakley Quick Mode  
Flags : 1 (ENCRYPT )  
Message ID : f2a6ce35  
Length : 52

1421 12/05/2001 11:40:54.250 SEV=8 IKEDBG/0 RPT=5357 172.18.124.241  
RECEIVED Message (msgid=f2a6ce35) with payloads :  
HDR + HASH (8) + NONE (0) ... total length : 48

1423 12/05/2001 11:40:54.250 SEV=9 IKEDBG/0 RPT=5358 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
processing hash

1424 12/05/2001 11:40:54.250 SEV=9 IKEDBG/0 RPT=5359 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
loading all IPSEC SAs

1425 12/05/2001 11:40:54.250 SEV=9 IKEDBG/1 RPT=671 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
Generating Quick Mode Key!

1426 12/05/2001 11:40:54.260 SEV=9 IKEDBG/1 RPT=672 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
Generating Quick Mode Key!

1427 12/05/2001 11:40:54.260 SEV=7 IKEDBG/0 RPT=5360 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
Loading subnet:  
Dst: 0.0.0.0 mask: 0.0.0.0  
Src: 172.18.124.217

1429 12/05/2001 11:40:54.260 SEV=4 IKE/49 RPT=58 172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
Security negotiation complete for User (esupporttcp)  
Responder, Inbound SPI = 0x70a4e243, Outbound SPI = 0x9879d238

1432 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/6 RPT=283  
IPSEC key message parse - msgtype 1, len 620, vers 1, pid 00000000,  
seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0,

spi 9879d238, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2,  
hmacAlg 3, lifetype 0, lifetime1 707832, lifetime2 0, dsId 0

1436 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1063  
Processing KEY\_ADD msg!

1437 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1064  
key\_msghdr2secassoc(): Enter

1438 12/05/2001 11:40:54.260 SEV=7 IPSECDBG/1 RPT=1065  
No USER filter configured

1439 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1066  
KeyProcessAdd: Enter

1440 12/05/2001 11:40:54.260 SEV=8 IPSECDBG/1 RPT=1067  
KeyProcessAdd: Adding outbound SA

1441 12/05/2001 11:40:54.260 SEV=8 IPSECDBG/1 RPT=1068  
KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, dst  
172.18.124.217 mask 0.0.0.0

1442 12/05/2001 11:40:54.260 SEV=8 IPSECDBG/1 RPT=1069  
KeyProcessAdd: FilterIpssecAddIkeSa success

1443 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/6 RPT=284  
IPSEC key message parse - msgtype 3, len 334, vers 1, pid 00000000,  
seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0,  
spi 70a4e243, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2,  
hmacAlg 3, lifetype 0, lifetime1 707832, lifetime2 0, dsId 0

1447 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1070  
Processing KEY\_UPDATE msg!

1448 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1071  
Update inbound SA addresses

1449 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1072  
key\_msghdr2secassoc(): Enter

1450 12/05/2001 11:40:54.260 SEV=7 IPSECDBG/1 RPT=1073  
No USER filter configured

1451 12/05/2001 11:40:54.260 SEV=9 IPSECDBG/1 RPT=1074  
KeyProcessUpdate: Enter

1452 12/05/2001 11:40:54.260 SEV=8 IPSECDBG/1 RPT=1075  
KeyProcessUpdate: success

1453 12/05/2001 11:40:54.260 SEV=8 IKEDBG/7 RPT=58  
IKE got a KEY\_ADD msg for SA: SPI = 0x9879d238

1454 12/05/2001 11:40:54.260 SEV=8 IKEDBG/0 RPT=5361  
pitcher: rcv KEY\_UPDATE, spi 0x70a4e243

1455 12/05/2001 11:40:54.260 SEV=4 IKE/120 RPT=58  
172.18.124.241  
Group [rtpvpn] User [esupporttcp]  
PHASE 2 COMPLETED (msgid=f2a6ce35)

1456 12/05/2001 11:40:55.120 SEV=7 IPSECDBG/1 RPT=1076  
IPSec Inbound SA has received data!

1457 12/05/2001 11:40:55.120 SEV=8 IKEDBG/0 RPT=5362

pitcher: recv KEY\_SA\_ACTIVE spi 0x709e5f39

1458 12/05/2001 11:40:55.120 SEV=8 IKEDBG/0 RPT=5363  
KEY\_SA\_ACTIVE no old rekey centry found with new spi  
0x709e5f39, mess\_id 0x0

## **Informations connexes**

- [Page d'assistance des concentrateurs VPN Cisco 3000](#)
- [Cisco VPN Client Support Page](#)
- [Page d'assistance IPsec](#)
- [Support et documentation techniques - Cisco Systems](#)