Exemple de configuration de L2TP sur IPsec entre Windows 2000 et le concentrateur VPN 3000 à l'aide de certificats numériques

Contenu

Introduction

Ce document affiche la procédure pas à pas utilisée pour se connecter à un concentrateur VPN 3000 d'un client de Windows 2000 utilisant le client de fonction intégrée L2TP/IPSec. On le suppose que vous utilisez les Certificats numériques (autorité de certification racine autonome (CA) sans inscription de certificat Protocol (le CÈPE)) pour authentifier votre connexion au concentrateur VPN. Ce document utilise le Microsoft Certificate Service pour l'illustration. Référez-vous au site Web de Microsoft pour la documentation sur la façon dont la configurer.

Remarque: C'est un exemple seulement parce que l'apparence des écrans de Windows 2000 peut changer.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont pour la gamme de concentrateurs de Cisco VPN 3000.

Objectifs

Dans cette procédure, vous vous terminez ces étapes :

1. Obtenez un certificat racine.
2. Obtenez un certificat d'identité pour le client.
3. Créez une connexion au VPN 3000 avec l'aide de l'assistant de connexion réseau.
4. Configurez le concentrateur VPN 3000.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Obtenez un certificat racine

Terminez-vous ces instructions afin d'obtenir un certificat racine :

1. Ouvrez une fenêtre du navigateur et saisissez l'URL pour le Microsoft Certificate Authority (habituellement http://servername ou l'adresse IP de CA/certsrv).La fenêtre bienvenue pour des récupérations de certificat et demande des affichages.
2. Sur la fenêtre bienvenue dessous sélectionnez une tâche, choisissez **récupèrent le certificat de CA ou la liste des révocations de certificat** et cliquent sur Next.
3. Du récupérer le certificat de CA ou la fenêtre de liste des révocations de certificat, clic **installent ce chemin de certification CA** dans le coin gauche.Ceci ajoute le certificat de CA à la mémoire de confiance d'autorités de certificat racine. Ceci signifie que tous les Certificats que ce CA fournit à ce client sont de confiance.

Obtenez un certificat d'identité pour le client

Terminez-vous ces étapes afin d'obtenir un certificat d'identité pour le client :

1. Ouvrez une fenêtre du navigateur et écrivez l'URL pour le Microsoft Certificate Authority (habituellement http://servername ou adresse IP de CA/certsrv).La fenêtre bienvenue pour des récupérations de certificat et demande des affichages.
2. De la fenêtre bienvenue, dessous sélectionnez une tâche, choisissez la **demande un certificat**, et cliquez sur Next.
3. De la fenêtre de type de requête de choisir, la **demande avancée** choisie et cliquent sur Next.
4. De la fenêtre avancée de demandes de certificat, choisie **soumettez une demande de certificat à ce CA utilisant une forme**.
5. Complétez le comme indiqué dans cet exemple de champs.La valeur pour le service (unité

organisationnelle) doit apparier le groupe configuré sur le concentrateur VPN. Ne spécifiez pas une taille de clé plus grande que 1024. Soyez sûr de sélectionner la case à cocher pour la **mémoire d'ordinateur local d'utilisation**. Quand vous êtes de finition, cliquez sur Next.Basé sur la façon dont le serveur CA est configuré, cette fenêtre apparaît parfois. S'il fait, contacter l'administrateur CA.

6. Cliquez sur **à la maison** pour revenir à l'écran principal, sélectionnez le **contrôle sur le certificat en suspens**, et cliquez sur Next.
7. Sur le certificat délivré la fenêtre, clic **installent ce certificat**.
8. Afin de visualiser votre certificat client, sélectionnez le **Start > Run**, et exécutez Microsoft Management Console (MMC).
9. Cliquez sur la **console** et choisissez l'**ajout/suppression SNAP-dans**.
10. Cliquez sur Add et choisissez le **certificat de la** liste.
11. Quand une fenêtre apparaît qui te demande la portée du certificat, choisissez le **compte d'ordinateur**.
12. Vérifiez que le certificat du serveur CA se trouve sous les Autorités de certification racine approuvée. Vérifiez également que vous avez un certificat en sélectionnant la **racine de console** > le **certificat (ordinateur local) > personnel** > des **Certificats**, suivant les indications de cette image.

Créez une connexion au VPN 3000 utilisant l'assistant de connexion réseau

Remplissez cette procédure afin de créer une connexion au VPN 3000 avec l'aide de l'assistant de connexion réseau :

1. Cliquez avec le bouton droit le **My Network Places**, choisissez Properties et le clic **établissent le nouveau rapport**.
2. De la fenêtre de type de connexion réseau, choisissez **se connectent à un réseau privé par l'Internet** et puis cliquent sur Next.
3. Écrivez le nom d'hôte ou l'adresse IP de l'interface publique du concentrateur VPN, et cliquez sur Next.
4. Sur la Disponibilité de fenêtre de connexion, sélectionnez **seulement pour me** et cliquez sur Next.
5. Sur la fenêtre de réseau public, sélectionnez si composer la connexion initiale (le compte ISP) automatiquement.
6. Sur l'écran d'adresse de destination, écrivez le nom d'hôte ou l'adresse IP du concentrateur VPN 3000, et cliquez sur Next.
7. Sur la fenêtre d'assistant de connexion réseau, écrivez un nom pour la connexion et cliquez sur Finish.Dans cet exemple, la connexion est nommée « Cisco VPN entreprise. »
8. Sur la fenêtre Connexion privée virtuelle, clic **Properties**.
9. Sur la fenêtre de Properties, sélectionnez l'onglet Mise en réseau.
10. Sous le type de serveur VPN que j'appelle, choisis **L2TP du** menu déroulant, mets en valeur le **TCP/IP d'Internet Protocol**, et clique sur **Properties**.
11. **Avancé** choisi **> options > Properties**.
12. Sur la fenêtre de sécurité IP, choisissez l'**utilisation cette stratégie de sécurité IP**.
13. Choisissez la stratégie de **client (répondez seulement) du** menu déroulant, et cliquez sur OK plusieurs fois jusqu'à ce que vous reveniez à l'écran de connecter.

14. Afin d'initier une connexion, écrire votre nom d'utilisateur et mot de passe, et clic **se connectent**.

Configurez le concentrateur VPN 3000

Obtenez un certificat racine

Terminez-vous ces étapes afin d'obtenir un certificat racine pour le concentrateur VPN 3000 :

1. Indiquez votre navigateur votre CA (habituellement quelque chose telle que http://ip_add_of_ca/certsrv/), **récupèrent le certificat de CA ou la liste des révocations de certificat**, et cliquent sur Next.
2. Cliquez sur Download le **certificat de CA** et sauvegardez le fichier quelque part sur votre disque local.
3. Sur le concentrateur VPN 3000, l'**Administration > Certificate Management** choisi, et le clic **ont cliquez ici pour installer un certificat** et **pour installer le certificat de CA**.
4. Cliquez sur Upload le **fichier du poste de travail**.
5. Cliquez sur **parcourent** et sélectionnent le fichier de certificat de CA que vous avez juste téléchargé.
6. Mettez en valeur le nom du fichier et le clic **installent**.

Obtenez un certificat d'identité pour le concentrateur VPN 3000

Terminez-vous ces étapes afin d'obtenir un certificat d'identité pour le concentrateur VPN 3000 :

1. **La Gestion** choisie de **ConfAdministration > de certificat > s'inscrivent > certificat d'identité**, puis cliquent sur **s'inscrivent par l'intermédiaire de la demande PKCS10 (manuel)**. Complétez la forme comme affiché ici et le clic **s'inscrivent**.Une fenêtre du navigateur s'affiche avec la demande de certificat. Il doit contenir le texte semblable à cette sortie :
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMDAwLW5hbWUxDDAKBgNVBAsTA3Nu
czEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAcTA2J4bDELMAkGA1UEBhMCYmUwWjAN
BgkqhkiG9w0BAQEFAANJADBGAkEAx7K+pvE004qILNNw3kPVWXrdlqZV4yeOIPdh
C8/V5Yuqq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG
SIb3DQEJDjElMCMwIQYDVR0RBBowGIIWdnBuMzAwMC1uYW1lLmNpc2NvLmNvbTAN
BgkqhkiG9w0BAQQFAANBABzcG3IKaWnDLFtrNf1QDi+D7w8dxPu74b/BRHn9fsKI
X6+X0ed0EuEgm1/2nfj8Ux0nV5F/c5wukUfysMmJ/ak=
-----END NEW CERTIFICATE REQUEST-----
```
2. Indiquez votre navigateur votre serveur CA, vérifiez la **demande un certificat**, et cliquez sur Next.
3. Vérifiez la **demande avancée**, cliquez sur Next, et choisi **soumettez une demande de certificat utilisant un fichier PKCS encodé par base64 #10 ou une demande de renouvellement utilisant un fichier PKCS encodé par base64 #7**.
4. Cliquez sur **Next** (Suivant). Coupez-collez le texte de la demande de certificat affichée précédemment dans la zone de texte. Cliquez sur **Submit**.
5. Basé sur la façon dont le serveur CA est configuré, vous pouvez cliquer sur Download le **certificat de CA**. Ou car bientôt le certificat a été délivré par le CA, retournez à votre serveur CA et vérifiez le **contrôle sur un certificat en attente**.
6. Cliquez sur Next, sélectionnez votre demande, et cliquez sur Next de nouveau.

7. Cliquez sur Download le **certificat de CA**, et sauvegardez le fichier sur le disque local.
8. Sur le concentrateur VPN 3000, l'**Administration > Certificate Management** choisi **> installent,** et le clic **installent le certificat obtenu par l'intermédiaire de l'inscription**.Vous voyez alors votre demande en suspens avec un état de « en cours, » comme dans cette image.
9. Le clic **installent**, suivi du **fichier de téléchargement du poste de travail**.
10. Cliquez sur **parcourent** et sélectionnent le fichier qui contient votre certificat délivré par le CA.
11. Mettez en valeur le nom du fichier et le clic **installent**.
12. **Administration > Certificate Management** choisi. Un écran semblable à cette image apparaît.

Configurez un groupe pour les clients

Remplissez cette procédure afin de configurer un groupe pour les clients :

1. Afin d'assigner une plage disponible des adresses IP, indiquer un navigateur l'interface interne du concentrateur VPN 3000 et de la **configuration > du système > de la gestion d'adresses > des groupes** choisis **> ajoutent**.
2. Spécifiez une plage des adresses IP qui ne sont en conflit avec aucun autre périphérique sur le réseau intérieur, et cliquez sur Add.
3. Afin de dire le concentrateur VPN 3000 d'utiliser le groupe, la **configuration** choisie **> le système > la gestion d'adresses > l'affectation**, cochent la case de **pools d'adresses d'utilisation**, et cliquent sur Apply, comme dans cette image.

Configurez une proposition d'IKE

Terminez-vous ces étapes afin de configurer une proposition d'IKE :

1. Sélectionnez la **configuration > les protocoles de système > de Tunnellisation > l'IPSec > les propositions d'IKE**, cliquez sur Add et sélectionnez les paramètres, suivant les indications de cette image.
2. Cliquez sur Add, mettez en valeur la nouvelle proposition dans la colonne de droite, et le clic **lancent**.

Configurez SA

Remplissez cette procédure afin de configurer l'association de sécurité (SA) :

1. **Configuration > Gestion des stratégies > gestion de trafic > SA** et clic choisis **ESP-L2TP-TRANSPORT**.Si cette SA n'est pas disponible ou si vous l'utilisez pour un autre but, créez nouvelle SA semblable à celle-ci. Les différentes configurations pour SA sont acceptables. Changez ce paramètre basé sur votre stratégie de sécurité.
2. Sélectionnez le certificat numérique que vous avez configuré précédemment sous le menu déroulant de **certificat numérique**. Sélectionnez la proposition d'Échange de clés Internet (IKE) **IKE-for-win2k**.**Remarque:** Ce n'est pas obligatoire. Quand le client L2TP/IPSec se connecte au concentrateur VPN, toutes les propositions d'IKE configurées sous la colonne active de la **configuration de** page **> des protocoles de système > de Tunnellisation > de l'IPSec > des propositions d'IKE** sont essayées dans la commande.Cette image affiche la

configuration requise pour SA :

Configurez le groupe et l'utilisateur

Remplissez cette procédure afin de configurer le groupe et l'utilisateur :

1. **Configuration > User Management** choisi **> groupe de base**.
2. Sous l'onglet Général, assurez-vous que **L2TP au-dessus d'IPSec** est vérifié.
3. Sous l'onglet d'IPSec, sélectionnez **ESP-L2TP-TRANSPORT** SA.
4. Sous l'onglet PPTP/L2TP, décochez toutes les **options de chiffrement L2TP**.
5. **Le Configuration > User Management > les utilisateurs** choisis et cliquent sur Add.
6. Entrez le nom et le mot de passe que vous utilisez pour connecter de votre client de Windows 2000. Assurez-vous que vous sélectionnez le **groupe de base** sous la sélection de groupe.
7. Sous l'onglet Général, vérifiez le **L2TP au-dessus du** protocole de Tunnellisation d'**IPSec**.
8. Sous l'onglet d'IPSec, sélectionnez **ESP-L2TP-TRANSPORT** SA.
9. Sous l'onglet PPTP/L2TP, décochez toutes les **options de chiffrement L2TP**, et cliquez sur Add.Vous pouvez maintenant se connecter avec l'aide du client de Windows 2000 L2TP/IPSec.**Remarque:** Vous avez choisi de configurer le groupe de base pour recevoir la connexion du distant L2TP/IPSec. Il est également possible de configurer un groupe qui apparie le champ de l'unité d'organisation (OU) de SA pour recevoir la connexion entrante. La configuration est identique.

Informations de débogage

```
269 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3868 10.48.66.76
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7

271 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3869 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

274 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3870 10.48.66.76
Proposal # 1, Transform # 2, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

279 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3871 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

282 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3872 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES
```

```
285 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3873 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

288 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3874 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

291 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3875 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

294 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3876 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

297 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3877 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

300 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3878 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

303 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3879 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

306 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3880 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

309 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3881 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

312 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3882 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

315 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3883 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class DH Group:
```

```
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

318 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3884 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7

321 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3885 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

324 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3886 10.48.66.76
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

329 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3887 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

332 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3888 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

335 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3889 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

338 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3890 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

341 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3891 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

344 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3892 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

347 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3893 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2
```

```
350 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3894 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

353 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3895 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

356 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3896 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

358 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3897 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

361 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3898 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

364 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3899 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

367 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3900 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

370 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3901 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

372 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3902 10.48.66.76
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

377 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3903 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

380 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3904 10.48.66.76
```

```
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

383 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3905 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

386 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3906 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

389 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3907 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

392 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3908 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

395 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3909 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

398 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3910 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

401 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3911 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

404 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3912 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class Auth Method:
    Rcv'd: RSA signature with Certificates
    Cfg'd: Preshared Key

407 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3913 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

410 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3914 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2
```

```
413 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3915 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

416 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3916 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

419 02/15/2002 12:47:24.430 SEV=7 IKEDBG/28 RPT=20 10.48.66.76
IKE SA Proposal # 1, Transform # 4 acceptable
Matches global IKE entry # 16

420 02/15/2002 12:47:24.440 SEV=9 IKEDBG/0 RPT=3917 10.48.66.76
constructing ISA_SA for isakmp

421 02/15/2002 12:47:24.490 SEV=8 IKEDBG/0 RPT=3918 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 80

423 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3919 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

425 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3920 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

427 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3921 10.48.66.76
processing ke payload

428 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3922 10.48.66.76
processing ISA_KE

429 02/15/2002 12:47:24.540 SEV=9 IKEDBG/1 RPT=104 10.48.66.76
processing nonce payload

430 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3923 10.48.66.76
constructing ke payload

431 02/15/2002 12:47:24.600 SEV=9 IKEDBG/1 RPT=105 10.48.66.76
constructing nonce payload

432 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3924 10.48.66.76
constructing certreq payload

433 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3925 10.48.66.76
Using initiator's certreq payload data

434 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=61 10.48.66.76
constructing Cisco Unity VID payload

435 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=62 10.48.66.76
constructing xauth V6 VID payload

436 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=39 10.48.66.76
Send IOS VID

437 02/15/2002 12:47:24.600 SEV=9 IKEDBG/38 RPT=20 10.48.66.76
Constructing VPN 3000 spoofing IOS Vendor ID payload
```

```
(version: 1.0.0, capabilities: 20000001)

439 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=63 10.48.66.76
constructing VID payload

440 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=40 10.48.66.76
Send Altiga GW VID

441 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3926 10.48.66.76
Generating keys for Responder...

442 02/15/2002 12:47:24.610 SEV=8 IKEDBG/0 RPT=3927 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 229

445 02/15/2002 12:47:24.640 SEV=8 IKEDBG/0 RPT=3928 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + CERT_REQ (7) + NONE (0)
... total length : 1186

448 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=106 10.48.66.76
Processing ID

449 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3929 10.48.66.76
processing cert payload

450 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=107 10.48.66.76
processing RSA signature

451 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3930 10.48.66.76
computing hash

452 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3931 10.48.66.76
processing cert request payload

453 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3932 10.48.66.76
Storing cert request payload for use in MM msg 4

454 02/15/2002 12:47:24.650 SEV=9 IKEDBG/23 RPT=20 10.48.66.76
Starting group lookup for peer 10.48.66.76

455 02/15/2002 12:47:24.650 SEV=9 IKE/21 RPT=12 10.48.66.76
No Group found by matching IP Address of Cert peer 10.48.66.76

456 02/15/2002 12:47:24.650 SEV=9 IKE/20 RPT=12 10.48.66.76
No Group found by matching OU(s) from ID payload:
 ou=sns,

457 02/15/2002 12:47:24.650 SEV=9 IKE/0 RPT=12 10.48.66.76
Group [VPNC_Base_Group]
No Group name for IKE Cert session, defaulting to BASE GROUP

459 02/15/2002 12:47:24.750 SEV=7 IKEDBG/0 RPT=3933 10.48.66.76
Group [VPNC_Base_Group]
Found Phase 1 Group (VPNC_Base_Group)

460 02/15/2002 12:47:24.750 SEV=7 IKEDBG/14 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
Authentication configured for Internal

461 02/15/2002 12:47:24.750 SEV=9 IKEDBG/19 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
IKEGetUserAttributes: default domain = fenetwork.com
```

```
462 02/15/2002 12:47:24.770 SEV=5 IKE/79 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Validation of certificate successful
(CN=my_name, SN=6102861F000000000005)

464 02/15/2002 12:47:24.770 SEV=7 IKEDBG/0 RPT=3934 10.48.66.76
Group [VPNC_Base_Group]
peer ID type 9 received (DER_ASN1_DN)

465 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=108 10.48.66.76
Group [VPNC_Base_Group]
constructing ID

466 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3935 10.48.66.76
Group [VPNC_Base_Group]
constructing cert payload

467 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=109 10.48.66.76
Group [VPNC_Base_Group]
constructing RSA signature

468 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3936 10.48.66.76
Group [VPNC_Base_Group]
computing hash

469 02/15/2002 12:47:24.800 SEV=9 IKEDBG/46 RPT=64 10.48.66.76
Group [VPNC_Base_Group]
constructing dpd vid payload

470 02/15/2002 12:47:24.800 SEV=8 IKEDBG/0 RPT=3937 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) + NONE (0)
... total length : 1112

473 02/15/2002 12:47:24.800 SEV=4 IKE/119 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 1 COMPLETED

474 02/15/2002 12:47:24.800 SEV=6 IKE/121 RPT=4 10.48.66.76
Keep-alive type for this connection: None

475 02/15/2002 12:47:24.800 SEV=6 IKE/122 RPT=4 10.48.66.76
Keep-alives configured on but peer does not support keep-alives (type = None)

476 02/15/2002 12:47:24.800 SEV=7 IKEDBG/0 RPT=3938 10.48.66.76
Group [VPNC_Base_Group]
Starting phase 1 rekey timer: 21600000 (ms)

477 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3939 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 1108

480 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3940 10.48.66.76
Group [VPNC_Base_Group]
processing hash

481 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3941 10.48.66.76
Group [VPNC_Base_Group]
processing SA payload

482 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=110 10.48.66.76
Group [VPNC_Base_Group]
```

```
processing nonce payload

483 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=111 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

484 02/15/2002 12:47:24.810 SEV=5 IKE/25 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received remote Proxy Host data in ID Payload:
Address 10.48.66.76, Protocol 17, Port 1701

487 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=112 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

488 02/15/2002 12:47:24.810 SEV=5 IKE/24 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received local Proxy Host data in ID Payload:
Address 10.48.66.109, Protocol 17, Port 0

491 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3942
QM IsRekeyed old sa not found by addr

492 02/15/2002 12:47:24.810 SEV=5 IKE/66 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IKE Remote Peer configured for SA: ESP-L2TP-TRANSPORT

493 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3943 10.48.66.76
Group [VPNC_Base_Group]
processing IPSEC SA

494 02/15/2002 12:47:24.810 SEV=7 IKEDBG/27 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IPSec SA Proposal # 1, Transform # 1 acceptable

495 02/15/2002 12:47:24.810 SEV=7 IKEDBG/0 RPT=3944 10.48.66.76
Group [VPNC_Base_Group]
IKE: requesting SPI!

496 02/15/2002 12:47:24.810 SEV=8 IKEDBG/6 RPT=4
IKE got SPI from key engine: SPI = 0x10d19e33

497 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3945 10.48.66.76
Group [VPNC_Base_Group]
oakley constucting quick mode

498 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3946 10.48.66.76
Group [VPNC_Base_Group]
constructing blank hash

499 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3947 10.48.66.76
Group [VPNC_Base_Group]
constructing ISA_SA for ipsec

500 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=113 10.48.66.76
Group [VPNC_Base_Group]
constructing ipsec nonce payload

501 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=114 10.48.66.76
Group [VPNC_Base_Group]
constructing proxy ID

502 02/15/2002 12:47:24.820 SEV=7 IKEDBG/0 RPT=3948 10.48.66.76
Group [VPNC_Base_Group]
```

```
Transmitting Proxy Id:
  Remote host: 10.48.66.76  Protocol 17  Port 1701
  Local host:  10.48.66.109  Protocol 17  Port 0

506 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3949 10.48.66.76
Group [VPNC_Base_Group]
constructing qm hash

507 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3950 10.48.66.76
SENDING Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

510 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3951 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

512 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3952 10.48.66.76
Group [VPNC_Base_Group]
processing hash

513 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3953 10.48.66.76
Group [VPNC_Base_Group]
loading all IPSEC SAs

514 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=115 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

515 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=116 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

516 02/15/2002 12:47:24.830 SEV=7 IKEDBG/0 RPT=3954 10.48.66.76
Group [VPNC_Base_Group]
Loading host:
  Dst: 10.48.66.109
  Src: 10.48.66.76

517 02/15/2002 12:47:24.830 SEV=4 IKE/49 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Security negotiation complete for User ()
Responder, Inbound SPI = 0x10d19e33, Outbound SPI = 0x15895ab9

520 02/15/2002 12:47:24.830 SEV=8 IKEDBG/7 RPT=4
IKE got a KEY_ADD msg for SA: SPI = 0x15895ab9

521 02/15/2002 12:47:24.830 SEV=8 IKEDBG/0 RPT=3955
pitcher: rcv KEY_UPDATE, spi 0x10d19e33

522 02/15/2002 12:47:24.830 SEV=4 IKE/120 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 2 COMPLETED (msgid=781ceadc)

523 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3956
pitcher: recv KEY_SA_ACTIVE spi 0x10d19e33

524 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3957
KEY_SA_ACTIVE no old rekey centry found with new spi 0x10d19e33, mess_id 0x0
```

Dépannez les informations

Cette section montre quelques problèmes courants et les méthodes de dépannage pour chacun.

- Le serveur ne peut pas être démarré.Très probablement, le service d'IPSec n'est pas commencé. **Le Start > Programs > Administrative tools > le service** choisis et s'assurent que le **service d'IPSec** est activé.
- Erreur 786 : Aucun certificat valide d'ordinateur.Cette erreur indique un problème avec le certificat sur l'ordinateur local. Afin de regarder facilement votre certificat, sélectionnez le **Start > Run**, et exécutez le MMC. Cliquez sur la **console** et choisissez l'**ajout/suppression SNAP-dans**. Cliquez sur Add et choisissez le **certificat de la** liste. Quand une fenêtre apparaît qui te demande la portée du certificat, choisissez le **compte d'ordinateur**.Maintenant vous pouvez vérifier que le certificat du serveur CA se trouve sous les **Autorités de certification racine approuvée**. Vous pouvez également vérifier que vous avez un certificat en sélectionnant la **racine de console > le certificat (ordinateur local) > personnel > des Certificats**, suivant les indications de cette image.Cliquez sur le **certificat**. Vérifiez que tout est correct. Dans cet exemple, il y a une clé privée associée avec le certificat. Cependant, ce certificat a expiré. C'est la cause du problème.
- Erreur 792 : Délai d'attente de négociation de sécurité.Ce message apparaît après une longue période.Activez l'approprié met au point comme expliqué dans la Foire aux questions de concentrateur de Cisco VPN 3000. Lu par eux. Vous devez voir quelque chose semblable à cette sortie :
```
9337 02/15/2002 15:06:13.500 SEV=8 IKEDBG/0 RPT=7002 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

9340 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7003 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class Auth Method:
    Rcv'd: RSA signature with Certificates
    Cfg'd: Preshared Key

9343 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7004 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

9346 02/15/2002 15:06:13.510 SEV=7 IKEDBG/0 RPT=7005 10.48.66.76
All SA proposals found unacceptable

9347 02/15/2002 15:06:13.510 SEV=4 IKE/48 RPT=37 10.48.66.76
Error processing payload: Payload ID: 1

9348 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7006 10.48.66.76
IKE SA MM:261e40dd terminating:
flags 0x01000002, refcnt 0, tuncnt 0

9349 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7007
sending delete message
```
Ceci indique que la proposition d'IKE n'a pas été configurée correctement. Vérifiez les informations de configurer une section de proposition d'IKE de ce document.
- Erreur 789 : La couche de Sécurité rencontre une erreur de traitement.Activez l'approprié met au point comme expliqué dans la Foire aux questions de concentrateur de Cisco VPN 3000. Lu par eux. Vous devez voir quelque chose semblable à cette sortie :
```
11315 02/15/2002
15:36:32.030 SEV=8 IKEDBG/0 RPT=7686
Proposal # 1, Transform # 2, Type ESP, Id DES-CBC
Parsing received transform:
  Phase 2 failure:
```

```
  Mismatched attr types for class Encapsulation:
    Rcv'd: Transport
    Cfg'd: Tunnel

11320 02/15/2002 15:36:32.030 SEV=5 IKEDBG/0 RPT=7687
AH proposal not supported

11321 02/15/2002 15:36:32.030 SEV=4 IKE/0 RPT=27 10.48.66.76
Group [VPNC_Base_Group]
All IPSec SA proposals found unacceptable!
```

- Version utiliséeSurveillance > état du système choisis pour visualiser cette sortie :VPN

```
Concentrator Type: 3005
Bootcode Rev: Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 2000 05:36:41
Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Version 3.5.Rel Nov 27 2001 13:35:16
Up For: 44:39:48
Up Since: 02/13/2002 15:49:59
RAM Size: 32 MB
```

Informations connexes

- Support produit de Négociation IPSec/protocoles IKE
- Support technique - Cisco Systems