Configuration du client VPN Cisco sur le concentrateur VPN 3000 avec authentification SDI IPSec (serveur version 3.3)

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Informations générales
Configurez
Diagramme du réseau
Configurations
Vérifiez
Client VPN Cisco de test au concentrateur VPN 3000 avec le SDI
Dépannez
Activer l'élimination des imperfections sur le concentrateur VPN 3000
Bon debug d'IPSec avec l'authentification locale
Bon debug d'IPSec avec l'authentification locale
Bon debug avec le SDI
Debugs du mauvais
Informations connexes

Introduction

Le concentrateur de Cisco VPN 3000 peut être configuré pour authentifier des Clients VPN Cisco par un serveur d'International de dynamics de Sécurité (SDI). Le concentrateur VPN 3000 agit en tant que client de SDI, communiquant avec le serveur de SDI sur le port 5500 de Protocole UDP (User Datagram Protocol). Le document suivant affiche comment s'assurer que le serveur, le concentrateur VPN 3000, et le Client VPN Cisco de SDI fonctionnent correctement, et puis comment combiner les composants. Si votre concentrateur VPN 3000 n'a pas été encore configuré, utilisez les étapes de installent et configurent le concentrateur VPN 3000 sans SDI utilisant l'interface de ligne de commande (CLI) pour l'installation initiale et la configuration. Si votre concentrateur VPN 3000 a été précédemment configuré, suivez les étapes pour la configuration existante Modify (sans SDI).

Conditions préalables

Conditions requises

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Cette configuration a été développée et testée utilisant le logiciel et les versions de matériel ci-dessous.

- Serveur 3.3 de SDI (UNIX et NT)
- Concentrateur VPN 3000 (2.5.2)
- Client vpn 2.5.2.A

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

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

Informations générales

Ce document s'applique au Cisco VPN 3000 Client (2.5.x) ou au Client VPN Cisco (3.x). Avec la release de 3.0 et plus tard, vous pouvez maintenant configurer différents serveurs de SDI pour différents groupes par opposition à un serveur de SDI avez défini globalement et utilisé par tous les groupes. Ces groupes qui ne font pas configurer différents serveurs de SDI utiliseront le serveur de SDI défini globalement.

Il y a trois types de nouveaux modes du numéro d'identification personnel (PIN) dans le SDI. Le concentrateur VPN 3000 prend en charge les deux premières options comme affiché ci-dessous.

- L'utilisateur sélectionne le nouveau PIN.
- Le serveur sélectionne le nouveau PIN et informe des utilisateurs.
- Le serveur sélectionne le nouveau PIN et informe des utilisateurs ; les utilisateurs peuvent changer le PIN.

Configurez

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

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :

Configurations

Installez et configurez le concentrateur VPN 3000 sans SDI

Nous avons configuré le concentrateur VPN 3000 pour authentifier localement un utilisateur dans un groupe ; ce faisant, avant d'ajouter le SDI, nous pourrions déterminer qu'IPSec entre le Client VPN Cisco et le concentrateur VPN 3000 fonctionne. Nous avons effacé la configuration de concentrateur VPN 3000 sur le port de console en allant à la **gestion > réinitialisation > réinitialisation planification > réinitialisation de système avec l'usine/configuration par défaut**.

Après réinitialisation, la configuration initiale suivante a été faite :

Configuration du concentrateur de concentrateur VPN 3000

```
Login: admin Password: Welcome to Cisco Systems VPN 3000
Concentrator Series Command Line Interface Copyright (C)
1998-2000 Cisco Systems, Inc. -- : Set the time on your
device. The correct time is very important, -- : so that
logging and accounting entries are accurate. -- : Enter
the system time in the following format: -- : HH:MM:SS.
Example 21:30:00 for 9:30 PM > Time Quick -> [ 13:02:39
] -- : Enter the date in the following format. -- :
MM/DD/YYYY Example 06/12/1999 for June 12th 1999. > Date
Quick -> [ 10/09/2000 ] -- : Set the time zone on your
device. The correct time zone is very -- : important so
that logging and accounting entries are accurate. -- :
Enter the time zone using the hour offset from GMT: -- :
-12 : Kwajalein -11 : Samoa -10 : Hawaii -9 : Alaska --
: -8 : PST -7 : MST -6 : CST -5 : EST -- : -4 : Atlantic
-3 : Brasilia -2 : Mid-Atlantic -1 : Azores -- : 0 : GMT
+1 : Paris +2 : Cairo +3 : Kuwait -- : +4 : Abu Dhabi +5
: Karachi +6 : Almaty +7 : Bangkok -- : +8 : Singapore
+9 : Tokyo +10 : Sydney +11 : Solomon Is. -- : +12 :
Marshall Is. > Time Zone Quick -> [ -5 ] -5 1) Enable
DST Support 2) Disable DST Support Quick -> [ 1 ] This
table shows current IP addresses. Interface IP
Address/Subnet Mask MAC Address ----------------------
----------------------------------------------------
| Ethernet 1 - Private | 0.0.0.0/0.0.0.0 | | Ethernet 2
- Public | 0.0.0.0/0.0.0.0 | | Ethernet 3 - External |
0.0.0.0/0.0.0.0 | ----------------------------------
---------------------------------------- ** An address
is required for the private interface. ** > Enter IP
Address Quick Ethernet 1 -> [ 0.0.0.0 ] 10.31.1.59
Waiting for Network Initialization... > Enter Subnet
Mask Quick Ethernet 1 -> [ 255.0.0.0 ] 255.255.255.0 1)
Ethernet Speed 10 Mbps 2) Ethernet Speed 100 Mbps 3)
Ethernet Speed 10/100 Mbps Auto Detect Quick Ethernet 1
-> [ 3 ] 1) Enter Duplex - Half/Full/Auto 2) Enter
Duplex - Full Duplex 3) Enter Duplex - Half Duplex Quick
Ethernet 1 -> [ 1 ] 1) Modify Ethernet 1 IP Address
(Private) 2) Modify Ethernet 2 IP Address (Public) 3)
Modify Ethernet 3 IP Address (External) 4) Configure
Expansion Cards 5) Save changes to Config file 6)
Continue 7) Exit Quick -> 2 This table shows current IP
addresses. Interface IP Address/Subnet Mask MAC Address
----------------------------------------------------
---------------------- | Ethernet 1 - Private |
10.31.1.59/255.255.255.0 | 00.90.A4.00.1C.B4 | Ethernet
```

2 - Public | 0.0.0.0/0.0.0.0 | | Ethernet 3 - External | 0.0.0.0/0.0.0.0 | ---------- > Enter IP Address Quick Ethernet 2 -> [0.0.0.0] **172.18.124.134** > Enter Subnet Mask Quick Ethernet 2 -> [255.255.0.0] **255.255.255.0** 1) Ethernet Speed 10 Mbps 2) Ethernet Speed 100 Mbps 3) Ethernet Speed 10/100 Mbps Auto Detect Quick Ethernet 2 -> [3] 1) Enter Duplex - Half/Full/Auto 2) Enter Duplex - Full Duplex 3) Enter Duplex - Half Duplex Quick Ethernet 2 -> [1] 1) Modify Ethernet 1 IP Address (Private) 2) Modify Ethernet 2 IP Address (Public) 3) Modify Ethernet 3 IP Address (External) 4) Configure Expansion Cards 5) Save changes to Config file 6) Continue 7) Exit Quick -> 6 -- : Assign a system name to this device. > System Name Quick -> **vpn3000** -- : Specify a local DNS server, which lets you enter hostnames -- : rather than IP addresses while configuring. > DNS Server Quick -> [0.0.0.0] -- : Enter your Internet domain name; e.g., yourcompany.com > Domain Quick -> > Default Gateway Quick -> **172.18.124.1** -- : Configure protocols and encryption options. -- : This table shows current protocol settings PPTP | L2TP | ---------- | Enabled | Enabled | | No Encryption Req | No Encryption Req | ---------- 1) Enable PPTP 2) Disable PPTP Quick -> [1] 1) PPTP Encryption Required 2) No Encryption Required Quick -> [2] 1) Enable L2TP 2) Disable L2TP Quick -> [1] 1) L2TP Encryption Required 2) No Encryption Required Quick -> [2] 1) Enable IPSec 2) Disable IPSec Quick -> [1] -- : Configure address assignment for PPTP, L2TP and IPSec. 1) Enable Client Specified Address Assignment 2) Disable Client Specified Address Assignment Quick -> [2] 1) Enable Per User Address Assignment 2) Disable Per User Address Assignment Quick -> [2] 1) Enable DHCP Address Assignment 2) Disable DHCP Address Assignment Quick -> [2] 1) Enable Configured Pool Address Assignment 2) Disable Configured Pool Address Assignment Quick -> [2] **1** > Configured Pool Range Start Address Quick -> **192.168.1.1** > Configured Pool Range End Address Quick -> [0.0.0.0] **192.168.1.100** -- : Specify how to authenticate users 1) Internal Authentication Server 2) RADIUS Authentication Server 3) NT Domain Authentication Server 4) SDI Authentication Server 5) Continue Quick -> [1] **1** Current Users ---------- No Users ---------- 1) Add a User 2) Delete a User 3) Continue Quick -> **1** > User Name Quick -> **37297304** > Password Quick -> ********* Verify -> ********* Current Users ---------- | 1. 37297304 | | -------- ---------- 1) Add a User 2) Delete a User 3) Continue Quick -> **3** > IPSec Group Name Quick -> **vpn3000** > IPSec Group Password Quick -> ******** Verify -> ******** -- : We strongly recommend that you change the password for user admin. > Reset Admin Password Quick -> [*****] Verify -> 1) Goto Main Configuration Menu 2) Save changes to Config file 3) Exit Quick -> **2** 1) Goto Main Configuration Menu 2) Save changes to Config file 3) Exit Quick -> **3** Done

Modifiez la configuration existante (sans SDI)

Si le concentrateur VPN 3000 a été précédemment configuré, les écrans suivants sont utilisés pour vérifier le groupe, l'utilisateur, et les configurations IPSec/IKE :

1. Utilisez cet écran pour ajouter un groupe avec l'authentification locale :
2. Utilisez cet écran pour ajouter un utilisateur au groupe avec l'authentification locale :
3. Utilisez l'écran de proposition d'IPSec > d'IKE pour ajouter des configurations d'IKE (les configurations affichées sont les paramètres systèmes par défaut) :

Client VPN Cisco et concentrateur VPN 3000 de test sans SDI

Après avoir modifié la configuration existante sur le concentrateur VPN 3000, nous installons le Client VPN Cisco et avons configuré une nouvelle connexion pour nous terminer chez 172.18.124.134 (l'interface publique du concentrateur). Nos informations d'accès de groupe étaient "vpn3000" (le nom du groupe) et le mot de passe de groupe était le mot de passe pour le groupe. Quand nous avons cliqué sur **nous connectons**, le nom d'utilisateur était "37297304" (nom d'utilisateur) et le mot de passe utilisateur était le mot de passe pour l'utilisateur (enregistré localement sur le concentrateur VPN 3000 ; aucun SDI n'est impliqué pourtant). Voir le bon debug d'IPSec avec l'authentification locale pour l'IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE mettent au point.

Fonctionnement du serveur SDI de test sans concentrateur VPN 3000

UNIX (Solaris)

1. Sur le serveur de SDI, créez un compte sditest utilisant l'admintool de Solaris.L'entrée de /etc/passwd devrait ressembler à `:sditest:x:76:10::/local/0/sditest:/local/0/opt/ace/prog/sdshell` **Remarque:** Les valeurs et les chemins au répertoire home et au « sdshell » de l'utilisateur dépendent du système.
2. Assignez un jeton à sditest.
3. Essai Telnetting dans l'hôte UNIX comme sditest. L'hôte vous incite pour un mot de passe Unix et le CODE DE PASSAGE. Après avoir authentifié, il vous permet dedans comme sditest dans cet hôte.

NT de Microsoft Windows

1. Installez l'agent de SecurSight.
2. **Programmes** choisis **> SecurSight > test d'authentification**.

Configurez SDI/User pour parler au concentrateur VPN 3000

Employez les étapes suivantes pour configurer SDI/User pour parler au concentrateur VPN 3000 :

1. Sur le serveur de SDI éditez l'écran symbolique, vérifient que le jeton « est activé » et pas en nouveau mode PIN.
2. Le clic **resynchronisent le PIN de jeton** et de **positionnement à prochain Tokencode**.
3. Sur l'écran d'utilisateur d'éditer, assignez un jeton à l'utilisateur, et le vérifiez que « laissé créer un PIN » n'est pas vérifié.
4. Cliquez sur les lancements de client et les vérifiez que le concentrateur VPN 3000 est

inclus.**Remarque:** Le concentrateur VPN 3000 est considéré un client du serveur de SDI ; l'écran ci-dessous est l'écran de client d'Add/Edit de serveur de SDI. Puisque c'est un nouveau client, « le noeud envoyé » case secrète est grisé. Le serveur de SDI n'a pas eu l'occasion d'envoyer au « noeud » le fichier secret au concentrateur (ce fichier serait affiché dans le concentrateur dans la section d'**Administration > File Management > de fichiers** en tant que « SECURID »). Après une authentification réussie du VPN 3000, le fichier secret de « noeud » est affiché sur le concentrateur VPN 3000 et « le noeud envoyé » case secrète est coché.

5. Cliquez sur les **lancements d'utilisateur** et les vérifiez que l'utilisateur est inclus.

Configurez et testez le concentrateur VPN 3000 au SDI

Employez les étapes suivantes pour configurer et tester le concentrateur VPN 3000 au SDI.

1. Utilisez l'écran suivant pour configurer le concentrateur VPN 3000 pour authentifier au SDI :
2. **Du SDI**, allez à l'**état > au moniteur de log > au moniteur d'activité** et cliquez sur OK pour observer des demandes en entrée.
3. Sur le concentrateur VPN 3000, **test de** clic pour tester la connexion.
4. Si l'authentification est bonne, le concentrateur VPN 3000 affiche :**Authentification réussie**

Dans l'exemple ci-dessus, nous avons défini un serveur global de SDI. Nous pouvons également choisir de définir différents serveurs de SDI pour chaque groupe en allant au **Configuration > User Management > Groups**, mettant en valeur le groupe respectif, et en choisissant **modifiez le serveur authentique**.

Pour mettez au point les informations, se rapportent aux sections suivantes de ce document :

- Activer l'élimination des imperfections sur le concentrateur VPN 3000
- Bon debug avec le SDI
- Debugs du mauvais

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Client VPN Cisco de test au concentrateur VPN 3000 avec le SDI

Si tout fonctionne jusqu'à ce point, il est temps de combiner le Client VPN Cisco, le concentrateur VPN 3000, et le serveur de SDI. Nous devons apporter une modification sur le concentrateur VPN 3000 en modifiant le groupe de travail que nous avons appelé "vpn3000" pour envoyer des demandes au serveur de SDI.

Dépannez

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

Activer l'élimination des imperfections sur le concentrateur VPN 3000

Nom de classe pour l'authentification :

- AUTHENTIQUE
- AUTHDBG
- AUTHDECODE

Nom de classe pour IPSec :

- IKE, IKEDBG, IKEDECODE
- IPSEC, IPSECDBG, IPSECDECODE
- Sévérité pour se connecter = 1-9
- Sévérité pour consoler = 1-3

Le clic **obtiennent le log** pour visualiser les résultats de l'exécution de débogage.

Bon debug d'IPSec avec l'authentification locale

```
1 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=1 161.44.17.135
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
  Responder Cookie(8):  00 00 00 00 00 00 00 00
  Next Payload  :       SA (1)
  Exchange Type :       Oakley Aggressive Mode
  Flags         :       0
  Message ID    :       0
  Length        :       307

7 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=1 161.44.17.135
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + NONE (0)
... total length : 307

10 10/10/2000 17:12:32.560 SEV=9 IKEDBG/0 RPT=2 161.44.17.135
processing SA payload

11 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=2 161.44.17.135
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       120

14 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=3 161.44.17.135
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ISAKMP (1)
  #of Transforms:       4
  Spi           :       00 00 00 00
  Length        :       108

18 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=4 161.44.17.135
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       IKE (1)
  Length        :       24

20 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=5 161.44.17.135
Phase 1 SA Attribute Decode for Transform # 1:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       MD5 (1)
  DH Group      :       Oakley Group 1 (1)
  Auth Method   :       Preshared Key (1)
```

```
24 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=6 161.44.17.135
Transform # 2 Decode for Proposal # 1:
  Transform #   :       2
  Transform ID  :       IKE (1)
  Length        :       24

26 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=7 161.44.17.135
Phase 1 SA Attribute Decode for Transform # 2:
  Encryption Alg:       Triple-DES (5)
  Hash Alg      :       MD5 (1)
  DH Group      :       Oakley Group 1 (1)
  Auth Method   :       Preshared Key (1)

30 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=8 161.44.17.135
Transform # 3 Decode for Proposal # 1:
  Transform #   :       3
  Transform ID  :       IKE (1)
  Length        :       24

32 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=9 161.44.17.135
Phase 1 SA Attribute Decode for Transform # 3:
  Encryption Alg:       Triple-DES (5)
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 1 (1)
  Auth Method   :       Preshared Key (1)

36 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=10 161.44.17.135
Transform # 4 Decode for Proposal # 1:
  Transform #   :       4
  Transform ID  :       IKE (1)
  Length        :       24

38 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=11 161.44.17.135
Phase 1 SA Attribute Decode for Transform # 4:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 1 (1)
  Auth Method   :       Preshared Key (1)

42 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=3 161.44.17.135
Proposal # 1, Transform # 1, 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

47 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=4 161.44.17.135
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

50 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=5 161.44.17.135
Proposal # 1, Transform # 2, 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

55 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=6 161.44.17.135
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

60 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=7 161.44.17.135
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

62 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=8 161.44.17.135
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: Triple-DES
    Cfg'd: DES-CBC

65 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=9 161.44.17.135
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

70 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=10 161.44.17.135
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

73 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=11 161.44.17.135
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

75 10/10/2000 17:12:32.560 SEV=7 IKEDBG/0 RPT=12 161.44.17.135
Oakley proposal is acceptable

76 10/10/2000 17:12:32.560 SEV=9 IKEDBG/0 RPT=13 161.44.17.135
processing ke payload

77 10/10/2000 17:12:32.560 SEV=9 IKEDBG/0 RPT=14 161.44.17.135
processing ISA_KE

78 10/10/2000 17:12:32.560 SEV=9 IKEDBG/1 RPT=1 161.44.17.135
processing nonce payload

79 10/10/2000 17:12:32.560 SEV=9 IKEDBG/1 RPT=2 161.44.17.135
Processing ID

80 10/10/2000 17:12:32.560 SEV=9 IKEDBG/1 RPT=3 161.44.17.135
processing vid payload

81 10/10/2000 17:12:32.580 SEV=9 IKEDBG/23 RPT=1 161.44.17.135
Starting group lookup for peer 161.44.17.135

82 10/10/2000 17:12:32.680 SEV=7 IKEDBG/0 RPT=15 161.44.17.135
Found Phase 1 Group (vpn3000)

83 10/10/2000 17:12:32.680 SEV=7 IKEDBG/14 RPT=1 161.44.17.135
Authentication configured for Internal
```

```
84 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=16 161.44.17.135
constructing ISA_SA for isakmp

85 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=17 161.44.17.135
constructing ke payload

86 10/10/2000 17:12:32.680 SEV=9 IKEDBG/1 RPT=4 161.44.17.135
constructing nonce payload

87 10/10/2000 17:12:32.680 SEV=9 IKE/0 RPT=1 161.44.17.135
Generating keys for Responder...

88 10/10/2000 17:12:32.680 SEV=9 IKEDBG/1 RPT=5 161.44.17.135
constructing ID

89 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=18
construct hash payload

90 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=19 161.44.17.135
computing hash

91 10/10/2000 17:12:32.680 SEV=9 IKEDBG/1 RPT=6 161.44.17.135
constructing vid payload

92 10/10/2000 17:12:32.680 SEV=8 IKEDBG/0 RPT=20 161.44.17.135
SENDING Message (msgid=0) with payloads :
HDR + SA (1)  ... total length : 248

93 10/10/2000 17:12:32.730 SEV=8 IKEDECODE/0 RPT=12 161.44.17.135
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
  Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Aggressive Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       0
  Length        :       52

99 10/10/2000 17:12:32.730 SEV=8 IKEDBG/0 RPT=21 161.44.17.135
RECEIVED Message (msgid=0) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

101 10/10/2000 17:12:32.730 SEV=9 IKEDBG/0 RPT=22 161.44.17.135
processing hash

102 10/10/2000 17:12:32.730 SEV=9 IKEDBG/0 RPT=23 161.44.17.135
computing hash

103 10/10/2000 17:12:33.410 SEV=8 IKEDECODE/0 RPT=13 161.44.17.135
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
  Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       48687ca1
  Length        :       308

110 10/10/2000 17:12:33.410 SEV=9 IKEDBG/21 RPT=1 161.44.17.135
Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

111 10/10/2000 17:12:33.410 SEV=9 IKEDBG/0 RPT=24 161.44.17.135
constructing blank hash
```

```
112 10/10/2000 17:12:33.410 SEV=9 IKEDBG/0 RPT=25 161.44.17.135
constructing qm hash

113 10/10/2000 17:12:33.410 SEV=8 IKEDBG/0 RPT=26 161.44.17.135
SENDING Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8)  ... total length : 68

115 10/10/2000 17:12:44.680 SEV=8 IKEDECODE/0 RPT=14 161.44.17.135
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
  Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Transactional
  Flags         :       1   (ENCRYPT )
  Message ID    :       fc2ce5eb
  Length        :       92

122 10/10/2000 17:12:44.680 SEV=8 IKEDBG/0 RPT=27 161.44.17.135
RECEIVED Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 85

124 10/10/2000 17:12:44.680 SEV=9 IKEDBG/1 RPT=7
process_attr(): Enter!

125 10/10/2000 17:12:44.680 SEV=9 IKEDBG/1 RPT=8
Processing cfg reply attributes.

126 10/10/2000 17:12:44.980 SEV=7 IKEDBG/14 RPT=2 161.44.17.135
User [ 37297304 ]
Authentication configured for Internal

127 10/10/2000 17:12:44.980 SEV=4 IKE/52 RPT=7 161.44.17.135
User [ 37297304 ]
User (37297304) authenticated.

128 10/10/2000 17:12:44.980 SEV=9 IKEDBG/31 RPT=1 161.44.17.135
User [ 37297304 ]
Obtained IP addr (192.168.1.1) prior to initiating Mode Cfg (XAuth enabled)

130 10/10/2000 17:12:44.980 SEV=9 IKEDBG/0 RPT=28 161.44.17.135
User [ 37297304 ]
constructing blank hash

131 10/10/2000 17:12:44.980 SEV=9 IKEDBG/0 RPT=29 161.44.17.135
0000: 00010004 C0A80101 F0010000                ............

132 10/10/2000 17:12:44.980 SEV=9 IKEDBG/0 RPT=30 161.44.17.135
User [ 37297304 ]
constructing QM hash

133 10/10/2000 17:12:44.980 SEV=8 IKEDBG/0 RPT=31 161.44.17.135
SENDING Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8)  ... total length : 80

135 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=15 161.44.17.135
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
  Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Transactional
  Flags         :       1   (ENCRYPT )
  Message ID    :       fc2ce5eb
  Length        :       68
```

```
142 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=32 161.44.17.135
RECEIVED Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 64

144 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=9
process_attr(): Enter!

145 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=10
Processing cfg ACK attributes

146 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=11
Received IPV4 address ack!

147 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=12
Received Save PW ack!

148 10/10/2000 17:12:44.990 SEV=4 AUTH/21 RPT=18
User 37297304 connected

149 10/10/2000 17:12:44.990 SEV=7 IKEDBG/22 RPT=1 161.44.17.135
User [ 37297304 ]
Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

151 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=33 161.44.17.135
RECEIVED Message (msgid=48687ca1) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)
... total length : 304

154 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=34 161.44.17.135
User [ 37297304 ]
processing hash

155 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=35 161.44.17.135
User [ 37297304 ]
processing SA payload

156 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=16 161.44.17.135
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       180

159 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=17 161.44.17.135
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       99 15 18 B4
  Length        :       28

163 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=18 161.44.17.135
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       DES-CBC (2)
  Length        :       16

165 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=19 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
  HMAC Algorithm:       MD5 (1)
  Encapsulation :       Tunnel (1)

167 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=20 161.44.17.135
Proposal Decode:
```

```
  Proposal #    :       2
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       99 15 18 B4
  Length        :       28

171 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=21 161.44.17.135
Transform # 1 Decode for Proposal # 2:
  Transform #   :       1
  Transform ID  :       Triple-DES (3)
  Length        :       16

173 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=22 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
  HMAC Algorithm:       MD5 (1)
  Encapsulation :       Tunnel (1)

175 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=23 161.44.17.135
Proposal Decode:
  Proposal #    :       3
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       99 15 18 B4
  Length        :       28

179 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=24 161.44.17.135
Transform # 1 Decode for Proposal # 3:
  Transform #   :       1
  Transform ID  :       DES-CBC (2)
  Length        :       16

181 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=25 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
  HMAC Algorithm:       SHA (2)
  Encapsulation :       Tunnel (1)

183 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=26 161.44.17.135
Proposal Decode:
  Proposal #    :       4
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       99 15 18 B4
  Length        :       28

187 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=27 161.44.17.135
Transform # 1 Decode for Proposal # 4:
  Transform #   :       1
  Transform ID  :       Triple-DES (3)
  Length        :       16

189 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=28 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
  HMAC Algorithm:       SHA (2)
  Encapsulation :       Tunnel (1)

191 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=29 161.44.17.135
Proposal Decode:
  Proposal #    :       5
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       99 15 18 B4
  Length        :       28

195 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=30 161.44.17.135
```

```
Transform # 1 Decode for Proposal # 5:
  Transform #   :       1
  Transform ID  :       NULL (11)
  Length        :       16

197 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=31 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
  HMAC Algorithm:       MD5 (1)
  Encapsulation :       Tunnel (1)

199 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=32 161.44.17.135
Proposal Decode:
  Proposal #    :       6
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       99 15 18 B4
  Length        :       28

203 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=33 161.44.17.135
Transform # 1 Decode for Proposal # 6:
  Transform #   :       1
  Transform ID  :       NULL (11)
  Length        :       16

205 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=34 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
  HMAC Algorithm:       SHA (2)
  Encapsulation :       Tunnel (1)

207 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=13 161.44.17.135
User [ 37297304 ]
processing nonce payload

208 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=14 161.44.17.135
User [ 37297304 ]
Processing ID

209 10/10/2000 17:12:44.990 SEV=5 IKE/25 RPT=13 161.44.17.135
User [ 37297304 ]
Received remote Proxy Host data in ID Payload:
Address 161.44.17.135, Protocol 0, Port 0

212 10/10/2000 17:12:44.990 SEV=7 IKEDBG/1 RPT=15 161.44.17.135
User [ 37297304 ]
Modifying client proxy src address!

213 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=16 161.44.17.135
User [ 37297304 ]
Processing ID

214 10/10/2000 17:12:44.990 SEV=5 IKE/24 RPT=7 161.44.17.135
User [ 37297304 ]
Received local Proxy Host data in ID Payload:
Address 172.18.124.134, Protocol 0, Port 0

217 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=36 161.44.17.135
User [ 37297304 ]
Processing Notify payload

218 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=35 161.44.17.135
Notify Payload Decode :
  DOI           :       IPSEC (1)
  Protocol      :       ISAKMP (1)
  Message       :       Initial contact (24578)
```

```
  Spi           :       9D F3 34 FE 89 BF AA B2 B7 AD 34 D2 74 4D 05 DA
  Length        :       28

224 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=37
QM IsRekeyed old sa not found by addr

225 10/10/2000 17:12:44.990 SEV=5 IKE/66 RPT=13 161.44.17.135
User [ 37297304 ]
IKE Remote Peer configured for SA: ESP-3DES-MD5

226 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=38 161.44.17.135
User [ 37297304 ]
processing IPSEC SA

227 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=39
Proposal # 1, Transform # 1, Type ESP, Id DES-CBC
Parsing received transform:
  Phase 2 failure:
  Mismatched transform IDs for protocol ESP:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

232 10/10/2000 17:12:45.000 SEV=7 IKEDBG/27 RPT=1 161.44.17.135
User [ 37297304 ]
IPSec SA Proposal # 2, Transform # 1 acceptable

233 10/10/2000 17:12:45.000 SEV=7 IKEDBG/0 RPT=40 161.44.17.135
User [ 37297304 ]
IKE: requesting SPI!

234 10/10/2000 17:12:45.000 SEV=6 IKE/0 RPT=2
AM received unexpected event EV_ACTIVATE_NEW_SA in state AM_ACTIVE

235 10/10/2000 17:12:45.000 SEV=9 IPSECDBG/6 RPT=1
IPSEC key message parse - msgtype 6, len 164, vers 1, pid 00000000, seq 13,
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 300,
lifetime2 2000000000, dsId 2

239 10/10/2000 17:12:45.000 SEV=9 IPSECDBG/1 RPT=1
Processing KEY_GETSPI msg!

240 10/10/2000 17:12:45.000 SEV=7 IPSECDBG/13 RPT=1
Reserved SPI 1773955517

241 10/10/2000 17:12:45.000 SEV=8 IKEDBG/6 RPT=1
IKE got SPI from key engine: SPI = 0x69bc69bd

242 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=41 161.44.17.135
User [ 37297304 ]
oakley constructing quick mode

243 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=42 161.44.17.135
User [ 37297304 ]
constructing blank hash

244 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=43 161.44.17.135
User [ 37297304 ]
constructing ISA_SA for ipsec

245 10/10/2000 17:12:45.000 SEV=9 IKEDBG/1 RPT=17 161.44.17.135
User [ 37297304 ]
constructing ipsec nonce payload
```

```
246 10/10/2000 17:12:45.000 SEV=9 IKEDBG/1 RPT=18 161.44.17.135
User [ 37297304 ]
constructing proxy ID

247 10/10/2000 17:12:45.000 SEV=7 IKEDBG/0 RPT=44 161.44.17.135
User [ 37297304 ]
Transmitting Proxy Id:
  Remote host: 192.168.1.1  Protocol 0  Port 0
  Local host:  172.18.124.134  Protocol 0  Port 0

251 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=45 161.44.17.135
User [ 37297304 ]
constructing QM hash

252 10/10/2000 17:12:45.000 SEV=8 IKEDBG/0 RPT=46 161.44.17.135
SENDING Message (msgid=48687ca1) with payloads :
HDR + HASH (8)  ... total length : 136

254 10/10/2000 17:12:45.010 SEV=8 IKEDECODE/0 RPT=36 161.44.17.135
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
  Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       48687ca1
  Length        :       52

261 10/10/2000 17:12:45.010 SEV=8 IKEDBG/0 RPT=47 161.44.17.135
RECEIVED Message (msgid=48687ca1) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

263 10/10/2000 17:12:45.010 SEV=9 IKEDBG/0 RPT=48 161.44.17.135
User [ 37297304 ]
processing hash

264 10/10/2000 17:12:45.010 SEV=9 IKEDBG/0 RPT=49 161.44.17.135
User [ 37297304 ]
loading all IPSEC SAs

265 10/10/2000 17:12:45.010 SEV=9 IKEDBG/1 RPT=19 161.44.17.135
User [ 37297304 ]
Generating Quick Mode Key!

266 10/10/2000 17:12:45.010 SEV=9 IKEDBG/1 RPT=20 161.44.17.135
User [ 37297304 ]
Generating Quick Mode Key!

267 10/10/2000 17:12:45.020 SEV=7 IKEDBG/0 RPT=50 161.44.17.135
User [ 37297304 ]
Loading host:
  Dst: 172.18.124.134
  Src: 192.168.1.1

268 10/10/2000 17:12:45.020 SEV=4 IKE/49 RPT=13 161.44.17.135
User [ 37297304 ]
Security negotiation complete for User (37297304)
Responder, Inbound SPI = 0x69bc69bd, Outbound SPI = 0x991518b4

271 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/6 RPT=2
IPSEC key message parse - msgtype 1, Len 536, vers 1, pid 00000000, seq 0,
err 0, type 2, mode 1, state 64, label 0, pad 0, spi 991518b4, encrKeyLen 24,
hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 0,
lifetime2 0, dsId 2
```

```
274 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=2
Processing KEY_ADD MSG!

275 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=3
key_msghdr2secassoc(): Enter

276 10/10/2000 17:12:45.020 SEV=7 IPSECDBG/1 RPT=4
No USER filter configured

277 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=5
KeyProcessAdd: Enter

278 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=6
KeyProcessAdd: Adding outbound SA

279 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=7
KeyProcessAdd: src 172.18.124.134 mask 0.0.0.0, dst 192.168.1.1 mask 0.0.0.0

280 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=8
KeyProcessAdd: FilterIpsecAddIkeSa success

281 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/6 RPT=3
IPSEC key message parse - msgtype 3, Len 292, vers 1, pid 00000000, seq 0,
err 0, type 2, mode 1, state 32, label 0, pad 0, spi 69bc69bd, encrKeyLen 24,
hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 0,
lifetime2 0, dsId 2

284 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=9
Processing KEY_UPDATE MSG!

285 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=10
Update inbound SA addresses

286 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=11
key_msghdr2secassoc(): Enter

287 10/10/2000 17:12:45.020 SEV=7 IPSECDBG/1 RPT=12
No USER filter configured

288 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=13
KeyProcessUpdate: Enter
289 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=14
KeyProcessUpdate: success

290 10/10/2000 17:12:45.020 SEV=8 IKEDBG/7 RPT=1
IKE got a KEY_ADD MSG for SA: SPI = 0x991518b4

291 10/10/2000 17:12:45.020 SEV=8 IKEDBG/0 RPT=51
pitcher: rcv KEY_UPDATE, spi 0x69bc69bd
```

Bon debug d'IPSec avec l'authentification locale

```
1 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=1 161.44.17.135
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
  Responder Cookie(8):  00 00 00 00 00 00 00 00
  Next Payload  :       SA (1)
  Exchange Type :       Oakley Aggressive Mode
  Flags         :       0
  Message ID    :       0
  Length        :       307

7 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=1 161.44.17.135
```

```
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + NONE (0)
... total length : 307

10 10/10/2000 17:12:32.560 SEV=9 IKEDBG/0 RPT=2 161.44.17.135
processing SA payload

11 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=2 161.44.17.135
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       120

14 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=3 161.44.17.135
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ISAKMP (1)
  #of Transforms:       4
  Spi           :       00 00 00 00
  Length        :       108

18 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=4 161.44.17.135
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       IKE (1)
  Length        :       24

20 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=5 161.44.17.135
Phase 1 SA Attribute Decode for Transform # 1:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       MD5 (1)
  DH Group      :       Oakley Group 1 (1)
  Auth Method   :       Preshared Key (1)

24 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=6 161.44.17.135
Transform # 2 Decode for Proposal # 1:
  Transform #   :       2
  Transform ID  :       IKE (1)
  Length        :       24

26 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=7 161.44.17.135
Phase 1 SA Attribute Decode for Transform # 2:
  Encryption Alg:       Triple-DES (5)
  Hash Alg      :       MD5 (1)
  DH Group      :       Oakley Group 1 (1)
  Auth Method   :       Preshared Key (1)

30 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=8 161.44.17.135
Transform # 3 Decode for Proposal # 1:
  Transform #   :       3
  Transform ID  :       IKE (1)
  Length        :       24

32 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=9 161.44.17.135
Phase 1 SA Attribute Decode for Transform # 3:
  Encryption Alg:       Triple-DES (5)
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 1 (1)
  Auth Method   :       Preshared Key (1)

36 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=10 161.44.17.135
Transform # 4 Decode for Proposal # 1:
  Transform #   :       4
  Transform ID  :       IKE (1)
```

```
  Length        :       24

38 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=11 161.44.17.135
Phase 1 SA Attribute Decode for Transform # 4:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 1 (1)
  Auth Method   :       Preshared Key (1)

42 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=3 161.44.17.135
Proposal # 1, Transform # 1, 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

47 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=4 161.44.17.135
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

50 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=5 161.44.17.135
Proposal # 1, Transform # 2, 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

55 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=6 161.44.17.135
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

60 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=7 161.44.17.135
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

62 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=8 161.44.17.135
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: Triple-DES
    Cfg'd: DES-CBC

65 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=9 161.44.17.135
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

70 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=10 161.44.17.135
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES
```

```
73 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=11 161.44.17.135
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

75 10/10/2000 17:12:32.560 SEV=7 IKEDBG/0 RPT=12 161.44.17.135
Oakley proposal is acceptable

76 10/10/2000 17:12:32.560 SEV=9 IKEDBG/0 RPT=13 161.44.17.135
processing ke payload

77 10/10/2000 17:12:32.560 SEV=9 IKEDBG/0 RPT=14 161.44.17.135
processing ISA_KE

78 10/10/2000 17:12:32.560 SEV=9 IKEDBG/1 RPT=1 161.44.17.135
processing nonce payload

79 10/10/2000 17:12:32.560 SEV=9 IKEDBG/1 RPT=2 161.44.17.135
Processing ID

80 10/10/2000 17:12:32.560 SEV=9 IKEDBG/1 RPT=3 161.44.17.135
processing vid payload

81 10/10/2000 17:12:32.580 SEV=9 IKEDBG/23 RPT=1 161.44.17.135
Starting group lookup for peer 161.44.17.135

82 10/10/2000 17:12:32.680 SEV=7 IKEDBG/0 RPT=15 161.44.17.135
Found Phase 1 Group (vpn3000)

83 10/10/2000 17:12:32.680 SEV=7 IKEDBG/14 RPT=1 161.44.17.135
Authentication configured for Internal

84 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=16 161.44.17.135
constructing ISA_SA for isakmp

85 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=17 161.44.17.135
constructing ke payload

86 10/10/2000 17:12:32.680 SEV=9 IKEDBG/1 RPT=4 161.44.17.135
constructing nonce payload

87 10/10/2000 17:12:32.680 SEV=9 IKE/0 RPT=1 161.44.17.135
Generating keys for Responder...

88 10/10/2000 17:12:32.680 SEV=9 IKEDBG/1 RPT=5 161.44.17.135
constructing ID

89 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=18
construct hash payload

90 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=19 161.44.17.135
computing hash

91 10/10/2000 17:12:32.680 SEV=9 IKEDBG/1 RPT=6 161.44.17.135
constructing vid payload

92 10/10/2000 17:12:32.680 SEV=8 IKEDBG/0 RPT=20 161.44.17.135
SENDING Message (msgid=0) with payloads :
HDR + SA (1)  ... total length : 248

93 10/10/2000 17:12:32.730 SEV=8 IKEDECODE/0 RPT=12 161.44.17.135
ISAKMP HEADER :         ( Version 1.0 )
```

```
  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
  Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Aggressive Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       0
  Length        :       52

99 10/10/2000 17:12:32.730 SEV=8 IKEDBG/0 RPT=21 161.44.17.135
RECEIVED Message (msgid=0) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

101 10/10/2000 17:12:32.730 SEV=9 IKEDBG/0 RPT=22 161.44.17.135
processing hash

102 10/10/2000 17:12:32.730 SEV=9 IKEDBG/0 RPT=23 161.44.17.135
computing hash

103 10/10/2000 17:12:33.410 SEV=8 IKEDECODE/0 RPT=13 161.44.17.135
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
  Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       48687ca1
  Length        :       308

110 10/10/2000 17:12:33.410 SEV=9 IKEDBG/21 RPT=1 161.44.17.135
Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

111 10/10/2000 17:12:33.410 SEV=9 IKEDBG/0 RPT=24 161.44.17.135
constructing blank hash

112 10/10/2000 17:12:33.410 SEV=9 IKEDBG/0 RPT=25 161.44.17.135
constructing qm hash

113 10/10/2000 17:12:33.410 SEV=8 IKEDBG/0 RPT=26 161.44.17.135
SENDING Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8)  ... total length : 68

115 10/10/2000 17:12:44.680 SEV=8 IKEDECODE/0 RPT=14 161.44.17.135
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
  Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Transactional
  Flags         :       1   (ENCRYPT )
  Message ID    :       fc2ce5eb
  Length        :       92

122 10/10/2000 17:12:44.680 SEV=8 IKEDBG/0 RPT=27 161.44.17.135
RECEIVED Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 85

124 10/10/2000 17:12:44.680 SEV=9 IKEDBG/1 RPT=7
process_attr(): Enter!

125 10/10/2000 17:12:44.680 SEV=9 IKEDBG/1 RPT=8
Processing cfg reply attributes.

126 10/10/2000 17:12:44.980 SEV=7 IKEDBG/14 RPT=2 161.44.17.135
User [ 37297304 ]
Authentication configured for Internal
```

```
127 10/10/2000 17:12:44.980 SEV=4 IKE/52 RPT=7 161.44.17.135
User [ 37297304 ]
User (37297304) authenticated.

128 10/10/2000 17:12:44.980 SEV=9 IKEDBG/31 RPT=1 161.44.17.135
User [ 37297304 ]
Obtained IP addr (192.168.1.1) prior to initiating Mode Cfg (XAuth enabled)

130 10/10/2000 17:12:44.980 SEV=9 IKEDBG/0 RPT=28 161.44.17.135
User [ 37297304 ]
constructing blank hash

131 10/10/2000 17:12:44.980 SEV=9 IKEDBG/0 RPT=29 161.44.17.135
0000: 00010004 C0A80101 F0010000                ............

132 10/10/2000 17:12:44.980 SEV=9 IKEDBG/0 RPT=30 161.44.17.135
User [ 37297304 ]
constructing QM hash

133 10/10/2000 17:12:44.980 SEV=8 IKEDBG/0 RPT=31 161.44.17.135
SENDING Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8)  ... total length : 80

135 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=15 161.44.17.135
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
  Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Transactional
  Flags         :       1   (ENCRYPT )
  Message ID    :       fc2ce5eb
  Length        :       68

142 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=32 161.44.17.135
RECEIVED Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 64

144 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=9
process_attr(): Enter!

145 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=10
Processing cfg ACK attributes

146 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=11
Received IPV4 address ack!

147 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=12
Received Save PW ack!

148 10/10/2000 17:12:44.990 SEV=4 AUTH/21 RPT=18
User 37297304 connected

149 10/10/2000 17:12:44.990 SEV=7 IKEDBG/22 RPT=1 161.44.17.135
User [ 37297304 ]
Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

151 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=33 161.44.17.135
RECEIVED Message (msgid=48687ca1) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)
... total length : 304

154 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=34 161.44.17.135
User [ 37297304 ]
```

```
processing hash

155 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=35 161.44.17.135
User [ 37297304 ]
processing SA payload

156 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=16 161.44.17.135
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       180

159 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=17 161.44.17.135
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       99 15 18 B4
  Length        :       28

163 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=18 161.44.17.135
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       DES-CBC (2)
  Length        :       16

165 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=19 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
  HMAC Algorithm:       MD5 (1)
  Encapsulation :       Tunnel (1)

167 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=20 161.44.17.135
Proposal Decode:
  Proposal #    :       2
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       99 15 18 B4
  Length        :       28

171 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=21 161.44.17.135
Transform # 1 Decode for Proposal # 2:
  Transform #   :       1
  Transform ID  :       Triple-DES (3)
  Length        :       16

173 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=22 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
  HMAC Algorithm:       MD5 (1)
  Encapsulation :       Tunnel (1)

175 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=23 161.44.17.135
Proposal Decode:
  Proposal #    :       3
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       99 15 18 B4
  Length        :       28

179 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=24 161.44.17.135
Transform # 1 Decode for Proposal # 3:
  Transform #   :       1
  Transform ID  :       DES-CBC (2)
  Length        :       16
```

```
181 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=25 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
  HMAC Algorithm:       SHA (2)
  Encapsulation :       Tunnel (1)

183 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=26 161.44.17.135
Proposal Decode:
  Proposal #    :       4
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       99 15 18 B4
  Length        :       28

187 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=27 161.44.17.135
Transform # 1 Decode for Proposal # 4:
  Transform #   :       1
  Transform ID  :       Triple-DES (3)
  Length        :       16

189 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=28 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
  HMAC Algorithm:       SHA (2)
  Encapsulation :       Tunnel (1)

191 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=29 161.44.17.135
Proposal Decode:
  Proposal #    :       5
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       99 15 18 B4
  Length        :       28

195 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=30 161.44.17.135
Transform # 1 Decode for Proposal # 5:
  Transform #   :       1
  Transform ID  :       NULL (11)
  Length        :       16

197 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=31 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
  HMAC Algorithm:       MD5 (1)
  Encapsulation :       Tunnel (1)

199 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=32 161.44.17.135
Proposal Decode:
  Proposal #    :       6
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       99 15 18 B4
  Length        :       28

203 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=33 161.44.17.135
Transform # 1 Decode for Proposal # 6:
  Transform #   :       1
  Transform ID  :       NULL (11)
  Length        :       16

205 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=34 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
  HMAC Algorithm:       SHA (2)
  Encapsulation :       Tunnel (1)

207 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=13 161.44.17.135
User [ 37297304 ]
```

```
processing nonce payload

208 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=14 161.44.17.135
User [ 37297304 ]
Processing ID

209 10/10/2000 17:12:44.990 SEV=5 IKE/25 RPT=13 161.44.17.135
User [ 37297304 ]
Received remote Proxy Host data in ID Payload:
Address 161.44.17.135, Protocol 0, Port 0

212 10/10/2000 17:12:44.990 SEV=7 IKEDBG/1 RPT=15 161.44.17.135
User [ 37297304 ]
Modifying client proxy src address!

213 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=16 161.44.17.135
User [ 37297304 ]
Processing ID

214 10/10/2000 17:12:44.990 SEV=5 IKE/24 RPT=7 161.44.17.135
User [ 37297304 ]
Received local Proxy Host data in ID Payload:
Address 172.18.124.134, Protocol 0, Port 0

217 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=36 161.44.17.135
User [ 37297304 ]
Processing Notify payload

218 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=35 161.44.17.135
Notify Payload Decode :
  DOI           :       IPSEC (1)
  Protocol      :       ISAKMP (1)
  Message       :       Initial contact (24578)
  Spi           :       9D F3 34 FE 89 BF AA B2 B7 AD 34 D2 74 4D 05 DA
  Length        :       28

224 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=37
QM IsRekeyed old sa not found by addr

225 10/10/2000 17:12:44.990 SEV=5 IKE/66 RPT=13 161.44.17.135
User [ 37297304 ]
IKE Remote Peer configured for SA: ESP-3DES-MD5

226 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=38 161.44.17.135
User [ 37297304 ]
processing IPSEC SA

227 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=39
Proposal # 1, Transform # 1, Type ESP, Id DES-CBC
Parsing received transform:
  Phase 2 failure:
  Mismatched transform IDs for protocol ESP:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

232 10/10/2000 17:12:45.000 SEV=7 IKEDBG/27 RPT=1 161.44.17.135
User [ 37297304 ]
IPSec SA Proposal # 2, Transform # 1 acceptable

233 10/10/2000 17:12:45.000 SEV=7 IKEDBG/0 RPT=40 161.44.17.135
User [ 37297304 ]
IKE: requesting SPI!

234 10/10/2000 17:12:45.000 SEV=6 IKE/0 RPT=2
```

```
AM received unexpected event EV_ACTIVATE_NEW_SA in state AM_ACTIVE

235 10/10/2000 17:12:45.000 SEV=9 IPSECDBG/6 RPT=1
IPSEC key message parse - msgtype 6, len 164, vers 1, pid 00000000, seq 13,
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 300,
lifetime2 2000000000, dsId 2

239 10/10/2000 17:12:45.000 SEV=9 IPSECDBG/1 RPT=1
Processing KEY_GETSPI msg!

240 10/10/2000 17:12:45.000 SEV=7 IPSECDBG/13 RPT=1
Reserved SPI 1773955517

241 10/10/2000 17:12:45.000 SEV=8 IKEDBG/6 RPT=1
IKE got SPI from key engine: SPI = 0x69bc69bd

242 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=41 161.44.17.135
User [ 37297304 ]
oakley constructing quick mode

243 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=42 161.44.17.135
User [ 37297304 ]
constructing blank hash

244 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=43 161.44.17.135
User [ 37297304 ]
constructing ISA_SA for ipsec

245 10/10/2000 17:12:45.000 SEV=9 IKEDBG/1 RPT=17 161.44.17.135
User [ 37297304 ]
constructing ipsec nonce payload

246 10/10/2000 17:12:45.000 SEV=9 IKEDBG/1 RPT=18 161.44.17.135
User [ 37297304 ]
constructing proxy ID

247 10/10/2000 17:12:45.000 SEV=7 IKEDBG/0 RPT=44 161.44.17.135
User [ 37297304 ]
Transmitting Proxy Id:
  Remote host: 192.168.1.1  Protocol 0  Port 0
  Local host:  172.18.124.134  Protocol 0  Port 0

251 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=45 161.44.17.135
User [ 37297304 ]
constructing QM hash

252 10/10/2000 17:12:45.000 SEV=8 IKEDBG/0 RPT=46 161.44.17.135
SENDING Message (msgid=48687ca1) with payloads :
HDR + HASH (8)  ... total length : 136

254 10/10/2000 17:12:45.010 SEV=8 IKEDECODE/0 RPT=36 161.44.17.135
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
  Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       48687ca1
  Length        :       52

261 10/10/2000 17:12:45.010 SEV=8 IKEDBG/0 RPT=47 161.44.17.135
RECEIVED Message (msgid=48687ca1) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48
```

```
263 10/10/2000 17:12:45.010 SEV=9 IKEDBG/0 RPT=48 161.44.17.135
User [ 37297304 ]
processing hash

264 10/10/2000 17:12:45.010 SEV=9 IKEDBG/0 RPT=49 161.44.17.135
User [ 37297304 ]
loading all IPSEC SAs

265 10/10/2000 17:12:45.010 SEV=9 IKEDBG/1 RPT=19 161.44.17.135
User [ 37297304 ]
Generating Quick Mode Key!

266 10/10/2000 17:12:45.010 SEV=9 IKEDBG/1 RPT=20 161.44.17.135
User [ 37297304 ]
Generating Quick Mode Key!

267 10/10/2000 17:12:45.020 SEV=7 IKEDBG/0 RPT=50 161.44.17.135
User [ 37297304 ]
Loading host:
  Dst: 172.18.124.134
  Src: 192.168.1.1

268 10/10/2000 17:12:45.020 SEV=4 IKE/49 RPT=13 161.44.17.135
User [ 37297304 ]
Security negotiation complete for User (37297304)
Responder, Inbound SPI = 0x69bc69bd, Outbound SPI = 0x991518b4

271 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/6 RPT=2
IPSEC key message parse - msgtype 1, Len 536, vers 1, pid 00000000, seq 0,
err 0, type 2, mode 1, state 64, label 0, pad 0, spi 991518b4, encrKeyLen 24,
hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 0,
lifetime2 0, dsId 2

274 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=2
Processing KEY_ADD MSG!

275 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=3
key_msghdr2secassoc(): Enter

276 10/10/2000 17:12:45.020 SEV=7 IPSECDBG/1 RPT=4
No USER filter configured

277 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=5
KeyProcessAdd: Enter

278 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=6
KeyProcessAdd: Adding outbound SA

279 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=7
KeyProcessAdd: src 172.18.124.134 mask 0.0.0.0, dst 192.168.1.1 mask 0.0.0.0

280 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=8
KeyProcessAdd: FilterIpsecAddIkeSa success

281 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/6 RPT=3
IPSEC key message parse - msgtype 3, Len 292, vers 1, pid 00000000, seq 0,
err 0, type 2, mode 1, state 32, label 0, pad 0, spi 69bc69bd, encrKeyLen 24,
hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 0,
lifetime2 0, dsId 2

284 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=9
Processing KEY_UPDATE MSG!
```

```
285 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=10
Update inbound SA addresses

286 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=11
key_msghdr2secassoc(): Enter

287 10/10/2000 17:12:45.020 SEV=7 IPSECDBG/1 RPT=12
No USER filter configured

288 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=13
KeyProcessUpdate: Enter
289 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=14
KeyProcessUpdate: success

290 10/10/2000 17:12:45.020 SEV=8 IKEDBG/7 RPT=1
IKE got a KEY_ADD MSG for SA: SPI = 0x991518b4

291 10/10/2000 17:12:45.020 SEV=8 IKEDBG/0 RPT=51
pitcher: rcv KEY_UPDATE, spi 0x69bc69bd
```

Bon debug avec le SDI

Debug de SDI

Si réussi (première authentification sur le SDI)

```
10/06/2000   11:57:04/U   37297304/vpn3000            000037297304/37297304
372
10/06/2000   11:57:04/L   Node Secret Sent to Client   zekie.cisco.com
10/06/2000   15:57:05/U   37297304/vpn3000            000037297304/37297304
372
10/06/2000   11:57:05/U   PASSCODE Accepted            zekie.cisco.com
```

Si réussi (après la première authentification sur le SDI)

```
10/06/2000   16:06:09U    37297304/vpn3000            000037297304/37297304
372
10/06/2000   12:06:09L    PASSCODE Accepted            zekie.cisco.com
```

Debug de concentrateur VPN 3000 (sur le test)

Debug « nom de classe » pour l'authentification :

- AUTHENTIQUE
- AUTHDBG
- AUTHDECODE

```
4 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/1 RPT=1
AUTH_Open() returns 14

5 10/06/2000 14:09:25.000 SEV=7 AUTH/12 RPT=1
Authentication session opened: handle = 14

6 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/3 RPT=1
AUTH_PutAttrTable(14, 5a2aa0)

7 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/5 RPT=1
AUTH_Authenticate(14, e5187e0, 306bdc)

8 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/59 RPT=1
AUTH_BindServer(71e097c, 0, 0)
```

```
9 10/06/2000 14:09:25.000 SEV=9 AUTHDBG/69 RPT=1
Auth Server 649ab4 has been bound to ACB 71e097c, sessions = 1

10 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/65 RPT=1
AUTH_CreateTimer(71e097c, 0, 0)

11 10/06/2000 14:09:25.000 SEV=9 AUTHDBG/72 RPT=1
Reply timer created: handle = 490011

12 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/61 RPT=1
AUTH_BuildMsg(71e097c, 0, 0)

13 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/51 RPT=1
Sdi_Build(71e097c)

14 10/06/2000 14:09:25.010 SEV=8 AUTHDBG/64 RPT=1
AUTH_StartTimer(71e097c, 0, 0)

15 10/06/2000 14:09:25.010 SEV=9 AUTHDBG/73 RPT=1
Reply timer started: handle = 490011, timestamp = 8553930, timeout = 4000

16 10/06/2000 14:09:25.010 SEV=8 AUTHDBG/62 RPT=1
AUTH_SndRequest(71e097c, 0, 0)

17 10/06/2000 14:09:25.010 SEV=8 AUTHDBG/52 RPT=1

Sdi_Xmt(71e097c)

18 10/06/2000 14:09:25.010 SEV=9 AUTHDBG/71 RPT=1
xmit_cnt = 1

19 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/63 RPT=1
AUTH_RcvReply(71e097c, 0, 0)

20 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/53 RPT=1
Sdi_Rcv(71e097c)

21 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/66 RPT=1
AUTH_DeleteTimer(71e097c, 0, 0)

22 10/06/2000 14:09:26.080 SEV=9 AUTHDBG/74 RPT=1
Reply timer stopped: handle = 490011, timestamp = 8554037

23 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/58 RPT=1
AUTH_Callback(71e097c, 0, 0)

24 10/06/2000 14:09:26.080 SEV=6 AUTH/4 RPT=1
Authentication successful: handle = 14, server = 172.18.124.99, user = 37297304

25 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/2 RPT=1
AUTH_Close(14)

26 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/60 RPT=1
AUTH_UnbindServer(71e097c, 0, 0)

27 10/06/2000 14:09:26.080 SEV=9 AUTHDBG/70 RPT=1
Auth Server 649ab4 has been unbound from ACB 71e097c, sessions = 0

28 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/10 RPT=1
AUTH_Int_FreeAuthCB(71e097c)

29 10/06/2000 14:09:26.080 SEV=9 AUTHDBG/19 RPT=1
instance = 15, clone_instance = 0
```

```
30 10/06/2000 14:09:26.080 SEV=7 AUTH/13 RPT=1
Authentication session closed: handle = 14
```

Debugs du mauvais

Mauvais nom d'utilisateur ou utilisateur non lancé sur le client

Le SDI mettent au point

```
10/06/2000 16:30:21U junk/vpn3000
10/06/2000 12:30:21L User Not on Client zekie.cisco.com
```

Le VPN 3000 mettent au point

```
21 10/06/2000 14:20:06.310 SEV=3 AUTH/5 RPT=5
Authentication rejected: Reason = Unspecified
handle = 15, server = 172.18.124.99, user = junk
```

Bon nom d'utilisateur, mauvais code de passage

Le SDI mettent au point

```
10/06/2000 16:33:07U 37297304/vpn3000   000037297304/37297304 372
10/06/2000 12:33:07L ACCESS DENIED, PASSCODE Incorrect zekie.cisco.com
```

Le VPN 3000 mettent au point

```
249 10/06/2000 14:22:52.160 SEV=3 AUTH/5 RPT=6
Authentication rejected: Reason = Unspecified
handle = 16, server = 172.18.124.99, user = 37297304
```

Serveur de SDI inaccessible ou démon vers le bas

Le SDI mettent au point

Expositions rien (n'a pas reçu la demande)

Le VPN 3000 mettent au point

```
77 10/06/2000 14:28:55.600 SEV=4 AUTH/9 RPT=7
Authentication failed: Reason = Network error
handle = 17, server = 172.18.124.99, user = 37297304
```

VPN 3000 non configuré comme client sur la case de SDI

Le SDI mettent au point

```
10/06/2000 17:37:42U --/172.18.124.134 -->/
10/06/2000 13:36:42L Client Not Found   zekie.cisco.com
```

Le VPN 3000 mettent au point

```
113 10/06/2000 15:26:27.440 SEV=3 AUTH/5 RPT=8
Authentication rejected: Reason = Unspecified
handle = 21, server = 172.18.124.99, user = 37297304
```

Concentrateur VPN 3000 retiré en tant que client du serveur de SDI, alors re-ajouté lui

Le serveur de SDI jugé pour envoyer en bas du fichier SecureID pour remplacer l'ancien, mais le VPN 3000 a déjà eu ce fichier.

Message sur le SDI

```
10/06/2000 13:42:18L Node Verification Failed zekie.cisco.com
```

Le VPN 3000 mettent au point

```
21 10/06/2000 15:32:03.030 SEV=3 AUTH/5 RPT=9
Authentication rejected: Reason = Unspecified
handle = 22, server = 172.18.124.99, user = 37297304
```

Pour résoudre ce problème, supprimez le fichier SecureID sur le concentrateur VPN 3000 en allant à la **gestion > à la gestion de fichiers > aux fichiers > au SECURID > à l'effacement**. Sur le contre-essai, le concentrateur VPN 3000 reçoit le nouveau fichier du serveur de SDI. Si **éditez le client > le noeud envoyé la** case que **secrète** est grisée sur le SDI, le serveur de SDI ne pouvait pas se terminer l'échange. Une fois que le concentrateur VPN 3000 a le fichier SecureID, le **noeud envoyé** case **secrète** est coché/pas grisé.

Informations connexes

- Configuration du client VPN Cisco sur le concentrateur VPN 3000 avec authentification SDI IPSec 5.0 et version ultérieure
- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du Client VPN 3000 Series Cisco
- Page d'assistance IPsec
- Support technique - Cisco Systems