

Configuration d'un tunnel IPSec – entre un concentrateur Cisco VPN 3000 et un pare-feu Checkpoint 4.1

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Conventions](#)

[Configurez le concentrateur VPN 3000](#)

[Configurez le pare-feu Checkpoint 4.1](#)

[Vérifiez](#)

[Dépannez](#)

[Récapitulation de réseau](#)

[Debug de concentrateur VPN 3000](#)

[Debug de pare-feu Checkpoint 4.1](#)

[Exemple de sortie de débogage](#)

[Informations connexes](#)

Introduction

Il explique comment créer un tunnel IPSec avec des clés pré-partagées afin de joindre deux réseaux privés :

- Un réseau privé à l'intérieur du concentrateur de Cisco VPN 3000 (192.168.1.x).
- Un réseau privé à l'intérieur du pare-feu Checkpoint 4.1 (10.32.50.x).

On le suppose que le trafic de l'intérieur du concentrateur et de l'intérieur VPN que le point de reprise à l'Internet (représenté dans ce document par les réseaux 172.18.124.x) circule avant que cette configuration commence.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Concentrateur VPN 3000
- Version de logiciel 2.5.2.F de concentrateur VPN 3000
- Pare-feu Checkpoint 4.1

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

[Diagramme du réseau](#)

Ce document utilise la configuration réseau suivante :

[Conventions](#)

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

[Configurez le concentrateur VPN 3000](#)

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

1. **La configuration > les protocoles de système > de Tunnellisation > l'IPSec > les propositions** choisis d'**IKE > modifient** pour créer une proposition d'Échange de clés Internet (IKE) nommée « DES-SHA » avec le hachage d'Algorithme de hachage sûr (SHA), le Norme de chiffrement de données (DES), et le congé du groupe 1. de Diffie-Hellman la vie de temps au par défaut 86400 secondes.**Remarque:** La plage valide pour la vie d'IKE de concentrateur VPN est de 60-2147483647 secondes.
2. **Configuration > protocoles de système > de Tunnellisation > IPSec > propositions** choisis d'**IKE**. Sélectionnez le « DES-SHA » et le clic **lancent** pour lancer la proposition d'IKE.
3. **La configuration > les protocoles de système > de Tunnellisation > l'entre réseaux locaux** choisis d'**IPSec > ajoutent**. Installez un tunnel d'IPsec appelé le « to_checkpoint » avec l'adresse de point de reprise en tant que pair. Pour la clé pré-partagée, introduisez l'adresse réelle. Sous l'authentification, l'ESP/SHA/HMAC-160 choisi, et le DES-56 choisi pour le cryptage. Écrivez la proposition d'IKE (« DES-SHA » dans cet exemple), et les gens du pays et les réseaux distants.
4. **La configuration > la Gestion des stratégies > la gestion de trafic > les associations de sécurité** choisies > **modifient**. Vérifiez que le perfect forward secrecy **est désactivé** et laissez à la vie de temps d'IPsec au par défaut **28800** secondes.**Remarque:** La plage valide pour la vie d'IPsec de concentrateur VPN est de 60-2147483647 secondes.
5. Enregistrez la configuration.

[Configurez le pare-feu Checkpoint 4.1](#)

Terminez-vous ces étapes pour configurer le pare-feu Checkpoint 4.1.

1. Puisque l'IKE et les vies par défaut d'IPsec diffèrent entre les constructeurs, **Propriétés** choisi > **le cryptage** pour placer les durées de vie du point de contrôle pour être d'accord avec le concentrateur VPN se transfère. La vie d'IKE de par défaut de concentrateur VPN est de 86400 secondes (minutes =1440). La vie d'IPsec de par défaut de concentrateur VPN est de 28800 secondes.
2. Choisi **gérez > des objets de réseau > nouveau (ou éditez) > réseau** pour configurer l'objet pour (« cpinside ») le réseau interne derrière le point de reprise. Ceci devrait être conforme au « réseau distant » dans le concentrateur VPN.
3. Choisi **gérez > des objets de réseau > éditez** pour éditer l'objet pour point final de passerelle (point de reprise le « RTPCPVPN ») que le concentrateur VPN a dans son paramètre de pair. Sous l'emplacement, **interne** choisi. Pour le type, **passerelle** choisie. Sous des modules installés, vérifiez **VPN-1 et FireWall-1** et vérifiez la **station de Gestion**.
4. Choisi **gérez > des objets de réseau > nouveau (ou éditez) > réseau** pour configurer l'objet pour (« inside_cisco ») le réseau externe derrière le concentrateur VPN. Ceci devrait être conforme au réseau « local » dans le concentrateur VPN.
5. Choisi **gérez > des objets de réseau > nouveau > poste de travail** pour ajouter un objet pour (« cisco_endpoint ») la passerelle externe de concentrateur VPN. C'est interface la « publique » de concentrateur VPN. Sous l'emplacement, **externe** choisi. Pour le type, **passerelle** choisie. **Remarque:** Ne sélectionnez pas la case VPN-1/FireWall-1.
6. Choisi **gérez > des objets de réseau > éditez** pour éditer onglet VPN de point d'extrémité de passerelle avec point de contrôle (appelé le le « RTPCPVPN »). Sous le domaine, sélectionnez autre et puis sélectionnez l'intérieur du réseau de points de contrôle (appelé le « cpinside ») de la liste déroulante. Sous des structures de chiffrement définies, **l'IKE** choisi, et cliquent sur Edit alors.
7. Changez les propriétés IKE pour le chiffrement DES pour être d'accord avec le **DES-56** et **l'algorithme de chiffrement** sur le concentrateur VPN.
8. Changez les propriétés IKE au hachage SHA1 pour être d'accord avec l'algorithme **SHA/HMAC-160** dans le concentrateur VPN. Retirez le **mode agressif**. Le contrôle **prend en charge des sous-réseaux. Secret pré-partagé de** contrôle sous la méthode d'authentification. Ceci est conforme à l'authentification mode de concentrateur VPN, des clés pré-partagées.
9. Cliquez sur Edit les **secrets** pour placer la clé pré-partagée pour être d'accord avec la **clé pré-partagée de** concentrateur de l'effectif VPN. **netmask principal principal de netmask d'address address d'ISAKMP**
10. Choisi **gérez > des objets de réseau > éditez** pour éditer l'onglet VPN de « cisco_endpoint ». Sous le domaine, sélectionnez **autre**, et puis sélectionnez l'intérieur du réseau de Cisco (appelé le « inside_cisco »). Sous des structures de chiffrement définies, **l'IKE** choisi, et cliquent sur Edit alors.
11. Changez le chiffrement DES de propriétés IKE pour être d'accord avec le **DES-56**, **algorithme de chiffrement** sur le concentrateur VPN.
12. Changez les propriétés IKE au hachage SHA1 pour être d'accord avec l'algorithme **SHA/HMAC-160** dans le concentrateur VPN. Changez ces configurations : **Mode de DeselectAggressive**. Le contrôle **prend en charge des sous-réseaux. Secret pré-partagé de** contrôle sous la méthode d'authentification. Ceci est conforme à l'authentification mode de concentrateur VPN des clés pré-partagées.
13. Cliquez sur Edit les **secrets** pour placer la clé pré-partagée pour être d'accord avec la clé pré-partagée de concentrateur de l'effectif VPN.
14. Dans la fenêtre de l'éditeur de stratégie, insérez une règle avec la source et la destination en tant que le « inside_cisco » et « cpinside » (bidirectionnel). Placez Service=Any,

Action=Encrypt, et Track=Long.

15. Sous le titre d'action, cliquez sur l'icône verte chiffrement et choisi **éditez les propriétés** pour configurer des stratégies de chiffrement.
16. **L'IKE** choisi, et cliquent sur Edit alors.
17. Sur la fenêtre de propriétés IKE, changez ces propriétés pour être d'accord avec le concentrateur IPsec VPN transforme. Sous transformez, **cryptage + intégrité des données** choisis (**ESP**). L'algorithme de chiffrement devrait être **DES**, intégrité des données devrait être SHA1, et la passerelle homologue permise devrait être la passerelle Cisco externe (appelée le « cisco_endpoint »). Cliquez sur **OK**.
18. Après que vous configuriez le point de reprise, la **stratégie** choisie > **installent** sur le menu du point de contrôle pour faire les prendre effet les modifications.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

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

Récapitulation de réseau

Quand des réseaux intérieurs adjacents de multiple sont configurés dans le domaine de cryptage sur le point de reprise, le périphérique pourrait automatiquement les récapituler en ce qui concerne le trafic intéressant. Si le concentrateur VPN n'est pas configuré pour s'assortir, le tunnel est susceptible d'échouer. Par exemple, si les réseaux intérieurs de 10.0.0.0 /24 et de 10.0.1.0 /24 sont configurés pour être inclus dans le tunnel, ils pourraient être récapitulés à 10.0.0.0 /23.

Debug de concentrateur VPN 3000

Le concentrateur possible VPN met au point incluent l'IKE, IKEDBG, KEDECODE, IPSEC, IPSECDBG, IPSECDECODE. Ceci est installé dans la **configuration > le système > les événements > les classes**.

Vous pouvez visualiser met au point dans la **surveillance > le journal d'événements > obtenez le log**.

Monitoring > Sessions choisi pour surveiller le trafic de tunnel entre réseaux locaux.

La gestion choisie > gèrent des sessions > des sessions entre réseaux locaux > des actions - déconnectez-vous pour effacer le tunnel.

Debug de pare-feu Checkpoint 4.1

Remarque: C'était une installation de NT de Microsoft Windows. Puisque le [cheminement a été placé pour long dans la fenêtre de l'éditeur de stratégie](#), refusé le trafic devrait apparaître en rouge dans le visualiseur de log. Plus bavard mettez au point peut être obtenu avec :

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

et dans une autre fenêtre :

```
C:\WINNT\FW1\4.1\fwstart
```

Émettez ces commandes d'effacer SAS sur le point de reprise :

```
fw tab -t IKE_SA_table -x fw tab -t ISAKMP_ESP_table -x fw tab -t inbound_SPI -x fw tab -t
ISAKMP_AH_table -x
```

La réponse oui au sont vous sure ? demande.

Exemple de sortie de débogage

Concentrateur Cisco VPN 3000

```
1 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=180 172.18.124.157
```

```
ISAKMP HEADER :          ( Version 1.0 )
  Initiator Cookie(8):   EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  00 00 00 00 00 00 00 00
  Next Payload   :      SA (1)
  Exchange Type  :      Oakley Main Mode
  Flags          :      0
  Message ID    :      0
  Length        :      164
```

```
7 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=406 172.18.124.157
```

```
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 164
```

```
9 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=407 172.18.124.157
```

```
processing SA payload
```

```
10 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=181 172.18.124.157
```

```
SA Payload Decode :
  DOI          :      IPSEC (1)
  Situation    :      Identity Only (1)
  Length       :      92
```

```
13 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=182 172.18.124.157
```

```
Proposal Decode:
  Proposal #   :      1
  Protocol ID  :      ISAKMP (1)
  #of Transforms:    2
  Length       :      80
```

```
16 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=183 172.18.124.157
```

```
Transform # 1 Decode for Proposal # 1:
  Transform #   :      1
  Transform ID  :      IKE (1)
  Length        :      36
```

```
18 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=184 172.18.124.157
```

```
Phase 1 SA Attribute Decode for Transform # 1:
  Encryption Alg:    DES-CBC (1)
  Hash Alg         :    SHA (2)
  Auth Method      :    Preshared Key (1)
  DH Group         :    Oakley Group 2 (2)
  Life Time        :    86400 seconds
```

```
23 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=185 172.18.124.157
```

Transform # 2 Decode for Proposal # 1:

Transform # : 2
Transform ID : IKE (1)
Length : 36

25 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=186 172.18.124.157

Phase 1 SA Attribute Decode for Transform # 2:

Encryption Alg: DES-CBC (1)
Hash Alg : SHA (2)
Auth Method : Preshared Key (1)
DH Group : Oakley Group 1 (1)
Life Time : 86400 seconds

30 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=408 172.18.124.157

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 2
Cfg'd: Oakley Group 1

35 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=409 172.18.124.157

Phase 1 failure against global IKE proposal # 2:

Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

38 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=410 172.18.124.157

Phase 1 failure against global IKE proposal # 3:

Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

41 02/13/2001 14:21:28.530 SEV=7 IKEDBG/0 RPT=411 172.18.124.157

Oakley proposal is acceptable

42 02/13/2001 14:21:28.530 SEV=9 IKEDBG/1 RPT=107 172.18.124.157

processing vid payload

43 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=412 172.18.124.157

processing IKE SA

44 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=413 172.18.124.157

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 2
Cfg'd: Oakley Group 1

49 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=414 172.18.124.157

Phase 1 failure against global IKE proposal # 2:

Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

52 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=415 172.18.124.157

Phase 1 failure against global IKE proposal # 3:

Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

55 02/13/2001 14:21:28.530 SEV=7 IKEDBG/28 RPT=3 172.18.124.157

IKE SA Proposal # 1, Transform # 2 acceptable

Matches global IKE entry # 1

56 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=416 172.18.124.157
constructing ISA_SA for isakmp

57 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=417 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + SA (1) ... total length : 84

58 02/13/2001 14:21:28.630 SEV=8 IKEDECODE/0 RPT=187 172.18.124.157
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): EF 61 3C 27 07 74 1B 25
Responder Cookie(8): 24 18 40 A1 3B E4 95 26
Next Payload : KE (4)
Exchange Type : Oakley Main Mode
Flags : 0
Message ID : 0
Length : 152

64 02/13/2001 14:21:28.630 SEV=8 IKEDBG/0 RPT=418 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

66 02/13/2001 14:21:28.630 SEV=8 IKEDBG/0 RPT=419 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

68 02/13/2001 14:21:28.630 SEV=9 IKEDBG/0 RPT=420 172.18.124.157
processing ke payload

69 02/13/2001 14:21:28.630 SEV=9 IKEDBG/0 RPT=421 172.18.124.157
processing ISA_KE

70 02/13/2001 14:21:28.630 SEV=9 IKEDBG/1 RPT=108 172.18.124.157
processing nonce payload

71 02/13/2001 14:21:28.650 SEV=9 IKEDBG/0 RPT=422 172.18.124.157
constructing ke payload

72 02/13/2001 14:21:28.650 SEV=9 IKEDBG/1 RPT=109 172.18.124.157
constructing nonce payload

73 02/13/2001 14:21:28.650 SEV=9 IKEDBG/38 RPT=7 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

75 02/13/2001 14:21:28.650 SEV=9 IKEDBG/1 RPT=110 172.18.124.157
constructing vid payload

76 02/13/2001 14:21:28.650 SEV=9 IKE/0 RPT=26 172.18.124.157
Generating keys for Responder...

77 02/13/2001 14:21:28.650 SEV=8 IKEDBG/0 RPT=423 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4) ... total length : 192

78 02/13/2001 14:21:28.770 SEV=8 IKEDECODE/0 RPT=188 172.18.124.157
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): EF 61 3C 27 07 74 1B 25
Responder Cookie(8): 24 18 40 A1 3B E4 95 26
Next Payload : ID (5)
Exchange Type : Oakley Main Mode
Flags : 1 (ENCRYPT)
Message ID : 0

Length : 68

84 02/13/2001 14:21:28.770 SEV=8 IKEDBG/0 RPT=424 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 64

86 02/13/2001 14:21:28.770 SEV=9 IKEDBG/1 RPT=111 172.18.124.157
Processing ID

87 02/13/2001 14:21:28.770 SEV=9 IKEDBG/0 RPT=425 172.18.124.157
processing hash

88 02/13/2001 14:21:28.770 SEV=9 IKEDBG/0 RPT=426 172.18.124.157
computing hash

89 02/13/2001 14:21:28.770 SEV=9 IKEDBG/23 RPT=7 172.18.124.157
Starting group lookup for peer 172.18.124.157

90 02/13/2001 14:21:28.870 SEV=7 IKEDBG/0 RPT=427 172.18.124.157
Found Phase 1 Group (172.18.124.157)

91 02/13/2001 14:21:28.870 SEV=7 IKEDBG/14 RPT=7 172.18.124.157
Authentication configured for Internal

92 02/13/2001 14:21:28.870 SEV=9 IKEDBG/1 RPT=112 172.18.124.157
constructing ID

93 02/13/2001 14:21:28.870 SEV=9 IKEDBG/0 RPT=428
construct hash payload

94 02/13/2001 14:21:28.870 SEV=9 IKEDBG/0 RPT=429 172.18.124.157
computing hash

95 02/13/2001 14:21:28.870 SEV=8 IKEDBG/0 RPT=430 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + ID (5) ... total length : 64

96 02/13/2001 14:21:28.870 SEV=7 IKEDBG/0 RPT=431 172.18.124.157
Starting phase 1 rekey timer

97 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=189 172.18.124.157
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): EF 61 3C 27 07 74 1B 25
Responder Cookie(8): 24 18 40 A1 3B E4 95 26
Next Payload : HASH (8)
Exchange Type : Oakley Quick Mode
Flags : 1 (ENCRYPT)
Message ID : 7755aa11
Length : 164

104 02/13/2001 14:21:29.030 SEV=8 IKEDBG/0 RPT=432 172.18.124.157
RECEIVED Message (msgid=7755aa11) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
th : 160

107 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=433 172.18.124.157
processing hash

108 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=434 172.18.124.157
processing SA payload

109 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=190 172.18.124.157
SA Payload Decode :

DOI : IPSEC (1)
Situation : Identity Only (1)
Length : 52

112 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=191 172.18.124.157

Proposal Decode:

Proposal # : 1
Protocol ID : ESP (3)
#of Transforms: 1
Spi : DA 16 3F E3
Length : 40

116 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=192 172.18.124.157

Transform # 1 Decode for Proposal # 1:

Transform # : 1
Transform ID : DES-CBC (2)
Length : 28

118 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=193 172.18.124.157

Phase 2 SA Attribute Decode for Transform # 1:

Life Time : 28800 seconds
HMAC Algorithm: SHA (2)
Encapsulation : Tunnel (1)

121 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=113 172.18.124.157

processing nonce payload

122 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=114 172.18.124.157

Processing ID

123 02/13/2001 14:21:29.030 SEV=5 IKE/35 RPT=14 172.18.124.157

Received remote IP Proxy Subnet data in ID Payload:

Address 10.32.50.0, Mask 255.255.255.0, Protocol 0, Port 0

125 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=115 172.18.124.157

Processing ID

126 02/13/2001 14:21:29.030 SEV=5 IKE/34 RPT=14 172.18.124.157

Received local IP Proxy Subnet data in ID Payload:

Address 192.168.1.0, Mask 255.255.255.0, Protocol 0, Port 0

128 02/13/2001 14:21:29.030 SEV=5 IKE/66 RPT=4 172.18.124.157

IKE Remote Peer configured for SA: L2L: to_checkpoint

129 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=435 172.18.124.157

processing IPSEC SA

130 02/13/2001 14:21:29.030 SEV=7 IKEDBG/27 RPT=1 172.18.124.157

IPSec SA Proposal # 1, Transform # 1 acceptable

131 02/13/2001 14:21:29.030 SEV=7 IKEDBG/0 RPT=436 172.18.124.157

IKE: requesting SPI!

132 02/13/2001 14:21:29.030 SEV=8 IKEDBG/6 RPT=6

IKE got SPI from key engine: SPI = 0x4d6e483f

133 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=437 172.18.124.157

oakley constructing quick mode

134 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=438 172.18.124.157

constructing blank hash

135 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=439 172.18.124.157

constructing ISA_SA for ipsec

136 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=116 172.18.124.157
constructing ipsec nonce payload

137 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=117 172.18.124.157
constructing proxy ID

138 02/13/2001 14:21:29.030 SEV=7 IKEDBG/0 RPT=440 172.18.124.157
Transmitting Proxy Id:
Remote subnet: 10.32.50.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 192.168.1.0 mask 255.255.255.0 Protocol 0 Port 0

141 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=441 172.18.124.157
constructing qm hash

142 02/13/2001 14:21:29.030 SEV=8 IKEDBG/0 RPT=442 172.18.124.157
SENDING Message (msgid=7755aa11) with payloads :
HDR + HASH (8) ... total length : 156

144 02/13/2001 14:21:29.270 SEV=8 IKEDECODE/0 RPT=194 172.18.124.157
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): EF 61 3C 27 07 74 1B 25
Responder Cookie(8): 24 18 40 A1 3B E4 95 26
Next Payload : HASH (8)
Exchange Type : Oakley Quick Mode
Flags : 1 (ENCRYPT)
Message ID : 7755aa11
Length : 60

151 02/13/2001 14:21:29.270 SEV=8 IKEDBG/0 RPT=443 172.18.124.157
RECEIVED Message (msgid=7755aa11) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 52

153 02/13/2001 14:21:29.270 SEV=9 IKEDBG/0 RPT=444 172.18.124.157
processing hash

154 02/13/2001 14:21:29.270 SEV=9 IKEDBG/0 RPT=445 172.18.124.157
loading all IPSEC SAs

155 02/13/2001 14:21:29.270 SEV=9 IKEDBG/1 RPT=118 172.18.124.157
Generating Quick Mode Key!

156 02/13/2001 14:21:29.270 SEV=9 IKEDBG/1 RPT=119 172.18.124.157
Generating Quick Mode Key!

157 02/13/2001 14:21:29.270 SEV=7 IKEDBG/0 RPT=446 172.18.124.157
Loading subnet:
Dst: 192.168.1.0 mask: 255.255.255.0
Src: 10.32.50.0 mask: 255.255.255.0

159 02/13/2001 14:21:29.270 SEV=4 IKE/49 RPT=6 172.18.124.157
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Responder, Inbound SPI = 0x4d6e483f, Outbound SPI = 0xda163fe3

161 02/13/2001 14:21:29.270 SEV=8 IKEDBG/7 RPT=6
IKE got a KEY_ADD msg for SA: SPI = 0xda163fe3

162 02/13/2001 14:21:29.270 SEV=8 IKEDBG/0 RPT=447
pitcher: rcv KEY_UPDATE, spi 0x4d6e483f

163 02/13/2001 14:21:29.670 SEV=8 IKEDECODE/0 RPT=195 172.18.124.157
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): EF 61 3C 27 07 74 1B 25
Responder Cookie(8): 24 18 40 A1 3B E4 95 26

Next Payload : HASH (8)
Exchange Type : Oakley Quick Mode
Flags : 1 (ENCRYPT)
Message ID : 7755aa11
Length : 60

170 02/13/2001 14:21:29.670 SEV=6 IKE/0 RPT=27 172.18.124.157
Duplicate Phase 2 packet detected!

171 02/13/2001 14:21:29.760 SEV=8 IKEDECODE/0 RPT=196 172.18.124.157
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): EF 61 3C 27 07 74 1B 25
Responder Cookie(8): 24 18 40 A1 3B E4 95 26
Next Payload : HASH (8)
Exchange Type : Oakley Quick Mode
Flags : 1 (ENCRYPT)
Message ID : 7755aa11
Length : 60

178 02/13/2001 14:21:29.760 SEV=6 IKE/0 RPT=28 172.18.124.157
Duplicate Phase 2 packet detected!

179 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=448
pitcher: recv KEY_SA_ACTIVE spi 0x4d6e483f

180 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=449
KEY_SA_ACTIVE old rekey centry found with new spi 0x4d6e483f

181 02/13/2001 14:21:29.880 SEV=7 IKEDBG/9 RPT=5 172.18.124.157
IKE Deleting SA: Remote Proxy 10.32.50.0, Local Proxy 192.168.1.0

182 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=450 172.18.124.157
IKE SA MM:f2ea8e68 rcv'd Terminate: state MM_ACTIVE_REKEY
flags 0x000000e6, refcnt 1, tuncnt 0

184 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=451 172.18.124.157
IKE SA MM:f2ea8e68 terminating:
flags 0x000000a6, refcnt 0, tuncnt 0

185 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=452
sending delete message

186 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=453 172.18.124.157
constructing blank hash

187 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=454
constructing delete payload

188 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=455 172.18.124.157
constructing qm hash

189 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=456 172.18.124.157
SENDING Message (msgid=87b7c1a4) with payloads :
HDR + HASH (8) ... total length : 80

191 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=457 172.18.124.157
IKE SA MM:241840a1 rcv'd Terminate: state MM_REKEY_DONE
flags 0x00000082, refcnt 1, tuncnt 1

193 02/13/2001 14:21:29.880 SEV=6 IKE/0 RPT=29 172.18.124.157
Removing peer from peer table failed, no match!

194 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=458
sending delete message

195 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=459 172.18.124.157
constructing blank hash

196 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=460
constructing ipsec delete payload

197 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=461 172.18.124.157
constructing qm hash

198 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=462 172.18.124.157
SENDING Message (msgid=63f2abb8) with payloads :
HDR + HASH (8) ... total length : 68

200 02/13/2001 14:21:29.880 SEV=7 IKEDBG/9 RPT=6 172.18.124.157
IKE Deleting SA: Remote Proxy 10.32.50.0, Local Proxy 192.168.1.0

201 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=463 172.18.124.157
IKE SA MM:241840a1 terminating:
flags 0x00000082, refcnt 0, tuncnt 0

202 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=464
sending delete message

203 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=465 172.18.124.157
constructing blank hash

204 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=466
constructing delete payload

205 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=467 172.18.124.157
constructing qm hash

206 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=468 172.18.124.157
SENDING Message (msgid=d6a00071) with payloads :
HDR + HASH (8) ... total length : 80

208 02/13/2001 14:21:29.880 SEV=4 AUTH/22 RPT=13
User 172.18.124.157 disconnected

209 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=469
pitcher: received key delete msg, spi 0x2962069b

210 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=470
pitcher: received key delete msg, spi 0xda163fe2

211 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=471
pitcher: received key delete msg, spi 0x4d6e483f

212 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=472
pitcher: received key delete msg, spi 0xda163fe3

213 02/13/2001 14:21:29.890 SEV=8 IKEDBG/0 RPT=473
pitcher: received a key acquire message!

214 02/13/2001 14:21:29.890 SEV=4 IKE/41 RPT=6 172.18.124.157
IKE Initiator: New Phase 1, Intf 2, IKE Peer 172.18.124.157
local Proxy Address 192.168.1.0, remote Proxy Address 10.32.50.0,
SA (L2L: to_checkpoint)

217 02/13/2001 14:21:29.890 SEV=9 IKEDBG/0 RPT=474 172.18.124.157
constructing ISA_SA for isakmp

218 02/13/2001 14:21:29.890 SEV=8 IKEDBG/0 RPT=475 172.18.124.157

SENDING Message (msgid=0) with payloads :
HDR + SA (1) ... total length : 84

219 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=197 172.18.124.157
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): FE 75 39 26 66 21 F6 F8
Responder Cookie(8): 67 1D 73 71 AE 2B 88 2E
Next Payload : SA (1)
Exchange Type : Oakley Main Mode
Flags : 0
Message ID : 0
Length : 84

225 02/13/2001 14:21:30.430 SEV=8 IKEDBG/0 RPT=476 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

227 02/13/2001 14:21:30.430 SEV=8 IKEDBG/0 RPT=477 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

229 02/13/2001 14:21:30.430 SEV=9 IKEDBG/0 RPT=478 172.18.124.157
processing SA payload

230 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=198 172.18.124.157
SA Payload Decode :
DOI : IPSEC (1)
Situation : Identity Only (1)
Length : 56

233 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=199 172.18.124.157
Proposal Decode:
Proposal # : 1
Protocol ID : ISAKMP (1)
#of Transforms: 1
Length : 44

236 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=200 172.18.124.157
Transform # 1 Decode for Proposal # 1:
Transform # : 1
Transform ID : IKE (1)
Length : 36

238 02/13/2001 14:21:30.440 SEV=8 IKEDECODE/0 RPT=201 172.18.124.157
Phase 1 SA Attribute Decode for Transform # 1:
Encryption Alg: DES-CBC (1)
Hash Alg : SHA (2)
DH Group : Oakley Group 1 (1)
Auth Method : Preshared Key (1)
Life Time : 86400 seconds

243 02/13/2001 14:21:30.440 SEV=7 IKEDBG/0 RPT=479 172.18.124.157
Oakley proposal is acceptable

244 02/13/2001 14:21:30.440 SEV=9 IKEDBG/0 RPT=480 172.18.124.157
constructing ke payload

245 02/13/2001 14:21:30.440 SEV=9 IKEDBG/1 RPT=120 172.18.124.157
constructing nonce payload

246 02/13/2001 14:21:30.440 SEV=9 IKEDBG/38 RPT=8 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

248 02/13/2001 14:21:30.440 SEV=9 IKEDBG/1 RPT=121 172.18.124.157
constructing vid payload

249 02/13/2001 14:21:30.440 SEV=8 IKEDBG/0 RPT=481 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4) ... total length : 192

250 02/13/2001 14:21:30.540 SEV=8 IKEDECODE/0 RPT=202 172.18.124.157
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): FE 75 39 26 66 21 F6 F8
Responder Cookie(8): 67 1D 73 71 AE 2B 88 2E
Next Payload : KE (4)
Exchange Type : Oakley Main Mode
Flags : 0
Message ID : 0
Length : 152

256 02/13/2001 14:21:30.540 SEV=8 IKEDBG/0 RPT=482 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

258 02/13/2001 14:21:30.540 SEV=8 IKEDBG/0 RPT=483 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

260 02/13/2001 14:21:30.540 SEV=9 IKEDBG/0 RPT=484 172.18.124.157
processing ke payload

261 02/13/2001 14:21:30.540 SEV=9 IKEDBG/0 RPT=485 172.18.124.157
processing ISA_KE

262 02/13/2001 14:21:30.540 SEV=9 IKEDBG/1 RPT=122 172.18.124.157
processing nonce payload

263 02/13/2001 14:21:30.560 SEV=9 IKE/0 RPT=30 172.18.124.157
Generating keys for Initiator...

264 02/13/2001 14:21:30.570 SEV=9 IKEDBG/1 RPT=123 172.18.124.157
constructing ID

265 02/13/2001 14:21:30.570 SEV=9 IKEDBG/0 RPT=486
construct hash payload

266 02/13/2001 14:21:30.570 SEV=9 IKEDBG/0 RPT=487 172.18.124.157
computing hash

267 02/13/2001 14:21:30.570 SEV=8 IKEDBG/0 RPT=488 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + ID (5) ... total length : 64

268 02/13/2001 14:21:30.740 SEV=8 IKEDECODE/0 RPT=203 172.18.124.157
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): FE 75 39 26 66 21 F6 F8
Responder Cookie(8): 67 1D 73 71 AE 2B 88 2E
Next Payload : ID (5)
Exchange Type : Oakley Main Mode
Flags : 1 (ENCRYPT)
Message ID : 0
Length : 68

274 02/13/2001 14:21:30.740 SEV=8 IKEDBG/0 RPT=489 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 64

276 02/13/2001 14:21:30.740 SEV=9 IKEDBG/1 RPT=124 172.18.124.157
Processing ID

277 02/13/2001 14:21:30.740 SEV=9 IKEDBG/0 RPT=490 172.18.124.157
processing hash

278 02/13/2001 14:21:30.740 SEV=9 IKEDBG/0 RPT=491 172.18.124.157
computing hash

279 02/13/2001 14:21:30.740 SEV=9 IKEDBG/23 RPT=8 172.18.124.157
Starting group lookup for peer 172.18.124.157

280 02/13/2001 14:21:30.830 SEV=8 IKEDECODE/0 RPT=204 172.18.124.157
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): FE 75 39 26 66 21 F6 F8
Responder Cookie(8): 67 1D 73 71 AE 2B 88 2E
Next Payload : ID (5)
Exchange Type : Oakley Main Mode
Flags : 1 (ENCRYPT)
Message ID : 0
Length : 68

286 02/13/2001 14:21:30.830 SEV=6 IKE/0 RPT=31 172.18.124.157
Duplicate Phase 1 packet detected!

287 02/13/2001 14:21:30.830 SEV=6 IKE/0 RPT=32
MM received unexpected event EV_RESEND_MSG in state MM_I_DONE

288 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=492 172.18.124.157
Found Phase 1 Group (172.18.124.157)

289 02/13/2001 14:21:30.840 SEV=7 IKEDBG/14 RPT=8 172.18.124.157
Authentication configured for Internal

290 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=493 172.18.124.157
Oakley begin quick mode

291 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=494 172.18.124.157
Starting phase 1 rekey timer

292 02/13/2001 14:21:30.840 SEV=4 AUTH/21 RPT=15
User 172.18.124.157 connected

293 02/13/2001 14:21:30.840 SEV=8 IKEDBG/6 RPT=7
IKE got SPI from key engine: SPI = 0x08201539

294 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=495 172.18.124.157
oakley constucting quick mode

295 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=496 172.18.124.157
constructing blank hash

296 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=497 172.18.124.157
constructing ISA_SA for ipsec

297 02/13/2001 14:21:30.840 SEV=9 IKEDBG/1 RPT=125 172.18.124.157
constructing ipsec nonce payload

298 02/13/2001 14:21:30.840 SEV=9 IKEDBG/1 RPT=126 172.18.124.157
constructing proxy ID

299 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=498 172.18.124.157
Transmitting Proxy Id:
Local subnet: 192.168.1.0 mask 255.255.255.0 Protocol 0 Port 0

Remote subnet: 10.32.50.0 Mask 255.255.255.0 Protocol 0 Port 0

302 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=499 172.18.124.157
constructing qm hash

303 02/13/2001 14:21:30.840 SEV=8 IKEDBG/0 RPT=500 172.18.124.157
SENDING Message (msgid=23bc1709) with payloads :
HDR + HASH (8) ... total length : 184

305 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=205 172.18.124.157
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): FE 75 39 26 66 21 F6 F8
Responder Cookie(8): 67 1D 73 71 AE 2B 88 2E
Next Payload : HASH (8)
Exchange Type : Oakley Quick Mode
Flags : 1 (ENCRYPT)
Message ID : 23bc1709
Length : 164

312 02/13/2001 14:21:31.000 SEV=8 IKEDBG/0 RPT=501 172.18.124.157
RECEIVED Message (msgid=23bc1709) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
th : 156

315 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=502 172.18.124.157
processing hash

316 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=503 172.18.124.157
processing SA payload

317 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=206 172.18.124.157
SA Payload Decode :
DOI : IPSEC (1)
Situation : Identity Only (1)
Length : 48

320 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=207 172.18.124.157
Proposal Decode:
Proposal # : 1
Protocol ID : ESP (3)
#of Transforms: 1
Spi : DA 16 3F E4
Length : 36

324 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=208 172.18.124.157
Transform # 1 Decode for Proposal # 1:
Transform # : 1
Transform ID : DES-CBC (2)
Length : 24

326 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=209 172.18.124.157
Phase 2 SA Attribute Decode for Transform # 1:
Life Time : 28800 seconds
Encapsulation : Tunnel (1)
HMAC Algorithm: SHA (2)

329 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=127 172.18.124.157
processing nonce payload

330 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=128 172.18.124.157
Processing ID

331 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=129 172.18.124.157
Processing ID

332 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=504 172.18.124.157
loading all IPSEC SAs

333 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=130 172.18.124.157
Generating Quick Mode Key!

334 02/13/2001 14:21:31.010 SEV=9 IKEDBG/1 RPT=131 172.18.124.157
Generating Quick Mode Key!

335 02/13/2001 14:21:31.010 SEV=7 IKEDBG/0 RPT=505 172.18.124.157
Loading subnet:
Dst: 10.32.50.0 mask: 255.255.255.0
Src: 192.168.1.0 mask: 255.255.255.0

337 02/13/2001 14:21:31.010 SEV=4 IKE/49 RPT=7 172.18.124.157
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Initiator, Inbound SPI = 0x08201539, Outbound SPI = 0xda163fe4

339 02/13/2001 14:21:31.010 SEV=9 IKEDBG/0 RPT=506 172.18.124.157
oakley constructing final quick mode

340 02/13/2001 14:21:31.010 SEV=8 IKEDBG/0 RPT=507 172.18.124.157
SENDING Message (msgid=23bc1709) with payloads :
HDR + HASH (8) ... total length : 76

342 02/13/2001 14:21:31.010 SEV=8 IKEDBG/7 RPT=7
IKE got a KEY_ADD msg for SA: SPI = 0xda163fe4

343 02/13/2001 14:21:31.010 SEV=8 IKEDBG/0 RPT=508
pitcher: rcv KEY_UPDATE, spi 0x8201539

344 02/13/2001 14:21:31.890 SEV=8 IKEDBG/0 RPT=509
pitcher: recv KEY_SA_ACTIVE spi 0x8201539

345 02/13/2001 14:21:31.890 SEV=8 IKEDBG/0 RPT=510
KEY_SA_ACTIVE no old rekey centry found with new spi 0x8201539, mess_id 0x0

[Informations connexes](#)

- [Négociation IPsec/Protocoles IKE](#)
- [Support et documentation techniques - Cisco Systems](#)