

IPSec トンネルの設定 - Cisco VPN 3000 コンセントレータから Checkpoint 4.1 Firewall へ

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[表記法](#)

[VPN 3000 コンセントレータの設定](#)

[Checkpoint 4.1 Firewallの設定](#)

[確認](#)

[トラブルシューティング](#)

[ネットワーク集約](#)

[VPN 3000 コンセントレータのデバッグ](#)

[Checkpoint 4.1 Firewall のデバッグ](#)

[debug 出力例](#)

[関連情報](#)

概要

このドキュメントでは、2つのプライベート ネットワークに参加するための、事前共有キーを使用した IPSec トンネルを構成する方法について説明します。

- Cisco VPN 3000 コンセントレータ(192.168.1.x)内のプライベートネットワーク。
- Checkpoint 4.1 Firewall(10.32.50.x)内のプライベートネットワーク。

この設定が開始される前に、VPN コンセントレータ内部およびチェックポイント内部からインターネット(このドキュメントでは172.18.124.x ネットワークで表される)へのトラフィックが流れることを前提としています。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

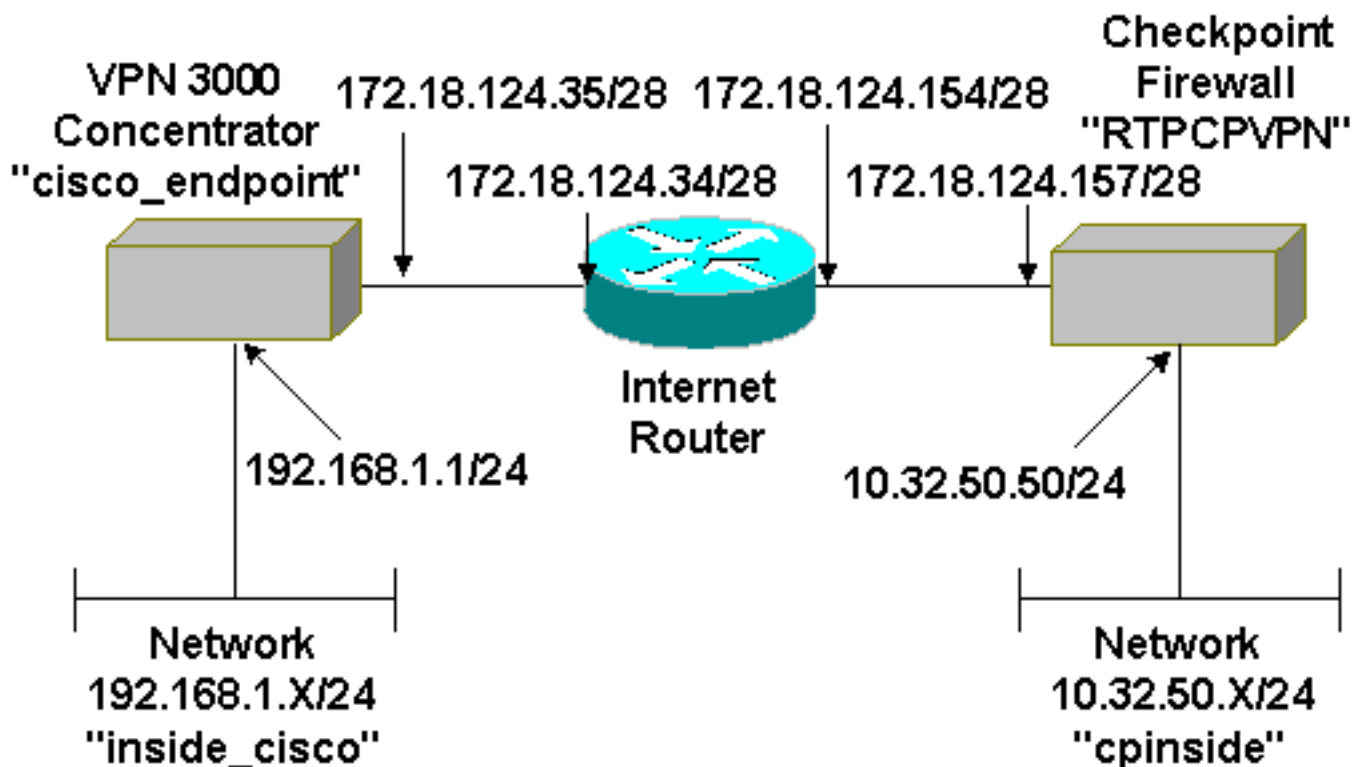
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- VPN 3000 コンセントレータ
- VPN 3000 コンセントレータ ソフトウェア リリース 2.5.2.F
- Checkpoint 4.1 Firewall

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



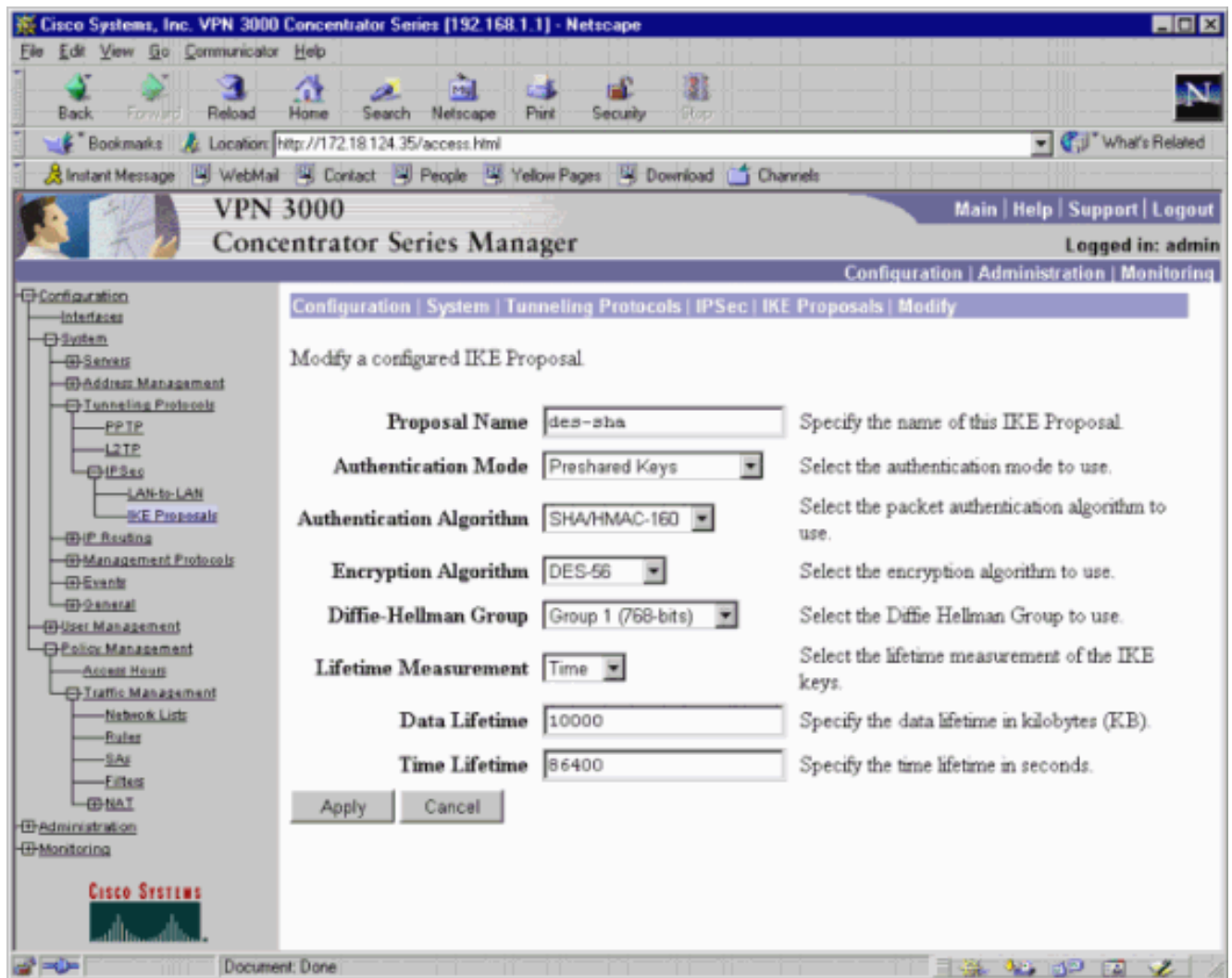
表記法

ドキュメント表記の詳細は、[『シスコテクニカルティップスの表記法』](#)を参照してください。

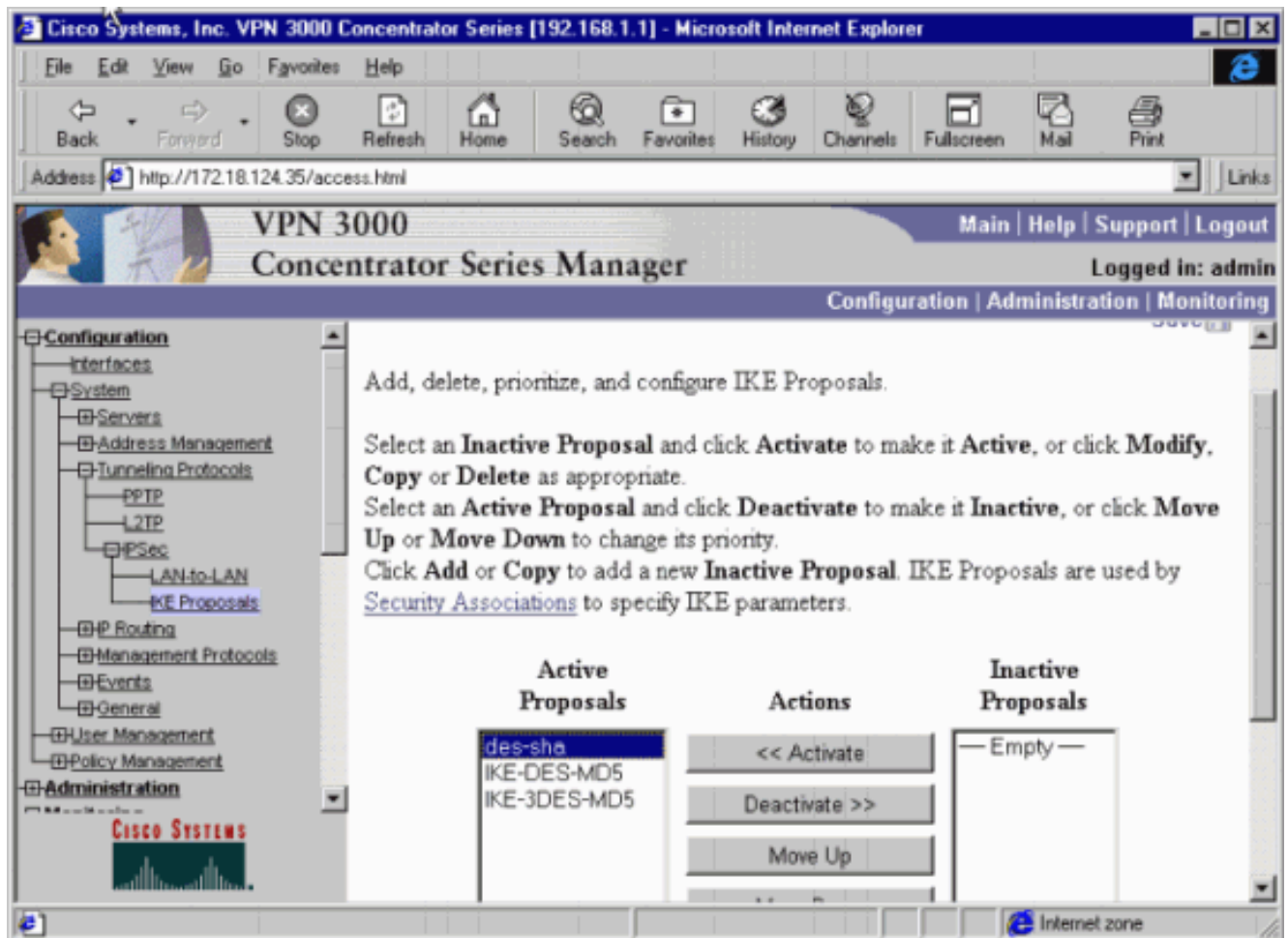
VPN 3000 コンセントレータの設定

VPN 3000 コンセントレータを設定するには、次の手順を実行します。

1. Configuration > System > Tunneling Protocols > IPSec > IKE Proposals > Modify の順に選択し、SHA ハッシュ、DES 暗号化、Diffie-Hellman Group 1 を指定した「des-sha」という名前の IKE プロポーザルを作成します。Time Lifetime はデフォルトの 86400 秒のままにしておきます。注：VPN コンセントレータの IKE ライフタイムの有効範囲は 60 ~ 2147483647 秒です。



2. Configuration > System > Tunneling Protocols > IPsec > IKE Proposals の順に選択します。「des-sha」を選択し、Activate をクリックして IKE プロポーザルをアクティブにします。



3. Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add の順に選択します。Checkpoint を付けた「to_checkpoint」という名前の IPSec トンネルを Peer として設定します。Preshared Key に、実際のキーを入力します。Authentication の下で ESP/SHA/HMAC-160 を選択し、Encryption で DES-56 を選択します。IKE プロポーザル（この例では「des-sha」）、Local Network、および Remote Network を入力します。

Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Location: http://172.18.124.35/access.html What's Related

Instant Message WebMail Contact People Yellow Pages Download Channels

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin


Configuration | Administration | Monitoring

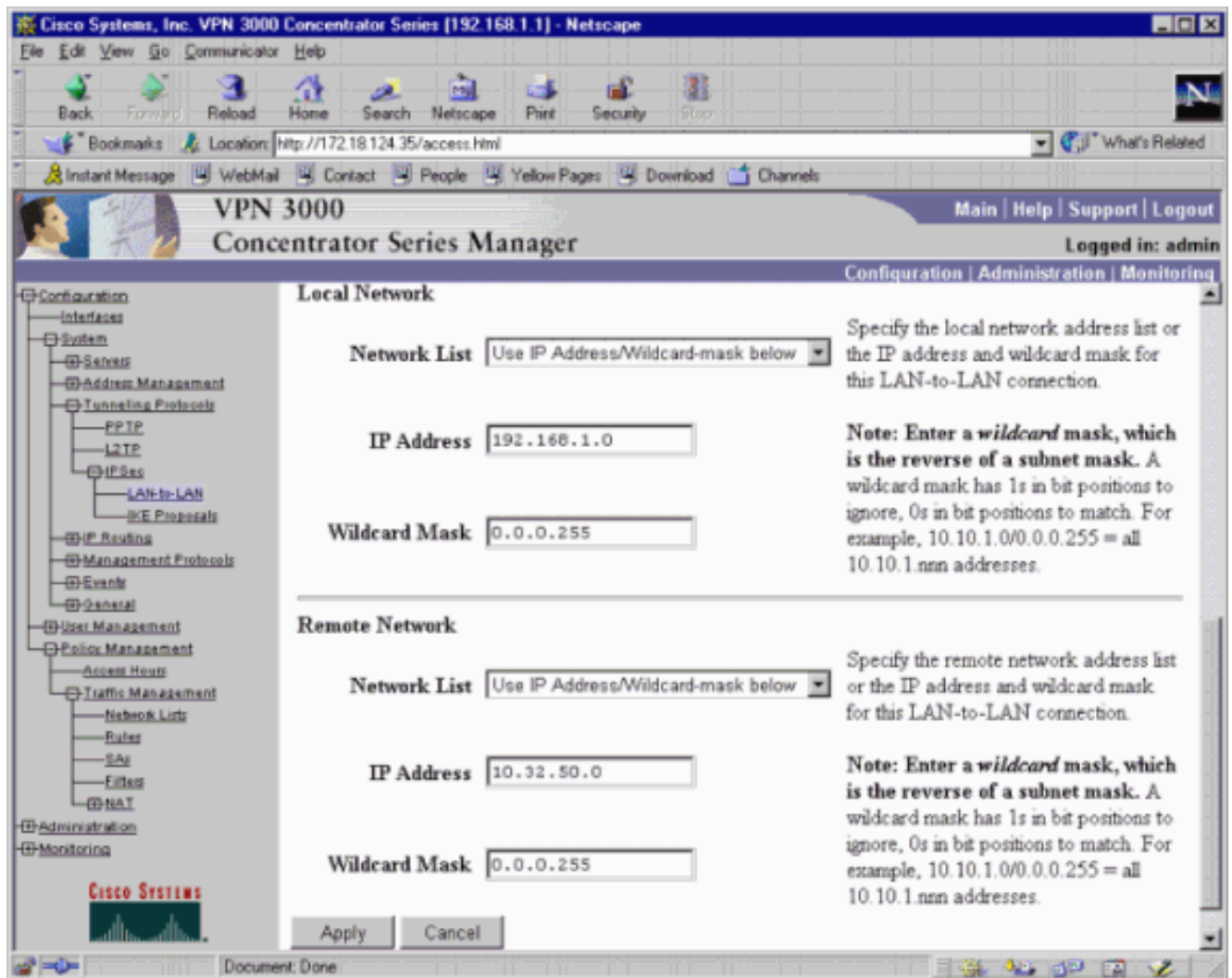
Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify

Modify an IPSec LAN-to-LAN connection.

Name	<input type="text" value="to_checkpoint"/>	Enter the name for this LAN-to-LAN connection.
Interface	<input type="text" value="Ethernet 2 (Public) (172.18.124.35)"/>	Select the interface to put this LAN-to-LAN connection on.
Peer	<input type="text" value="172.18.124.157"/>	Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Preshared Key	<input type="text" value="ciscorules"/>	Enter the preshared key for this LAN-to-LAN connection.
Authentication	<input type="text" value="ESP/SHA/HMAC-160"/>	Specify the packet authentication mechanism to use.
Encryption	<input type="text" value="DES-56"/>	Specify the encryption mechanism to use.
IKE Proposal	<input type="text" value="des-sha"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
Network Autodiscovery	<input type="checkbox"/>	Check to automatically discover networks. Parameters below are ignored if checked.

Access Hour Policies





4. Configuration > Policy Management > Traffic Management > Security Associations > Modify の順に選択します。Perfect Forward Secrecy が Disabled であることを確認し、IPsec の Time Lifetime をデフォルトの 28800 秒のままにします。注：VPNコンセントレータの IPsecライフタイムの有効範囲は60 ~ 2147483647秒です。

Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Location: http://172.18.124.35/access.html

Instant Message WebMail Contact People Yellow Pages Download Channels

VPN 3000
Concentrator Series Manager

Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association

SA Name Specify the name of this Security Association (SA).

Inheritance Select the granularity of this SA.

IPSec Parameters

Authentication Algorithm Select the packet authentication algorithm to use.

Encryption Algorithm Select the ESP encryption algorithm to use.

Encapsulation Mode Select the Encapsulation Mode for this SA.

Perfect Forward Secrecy Select the use of Perfect Forward Secrecy.

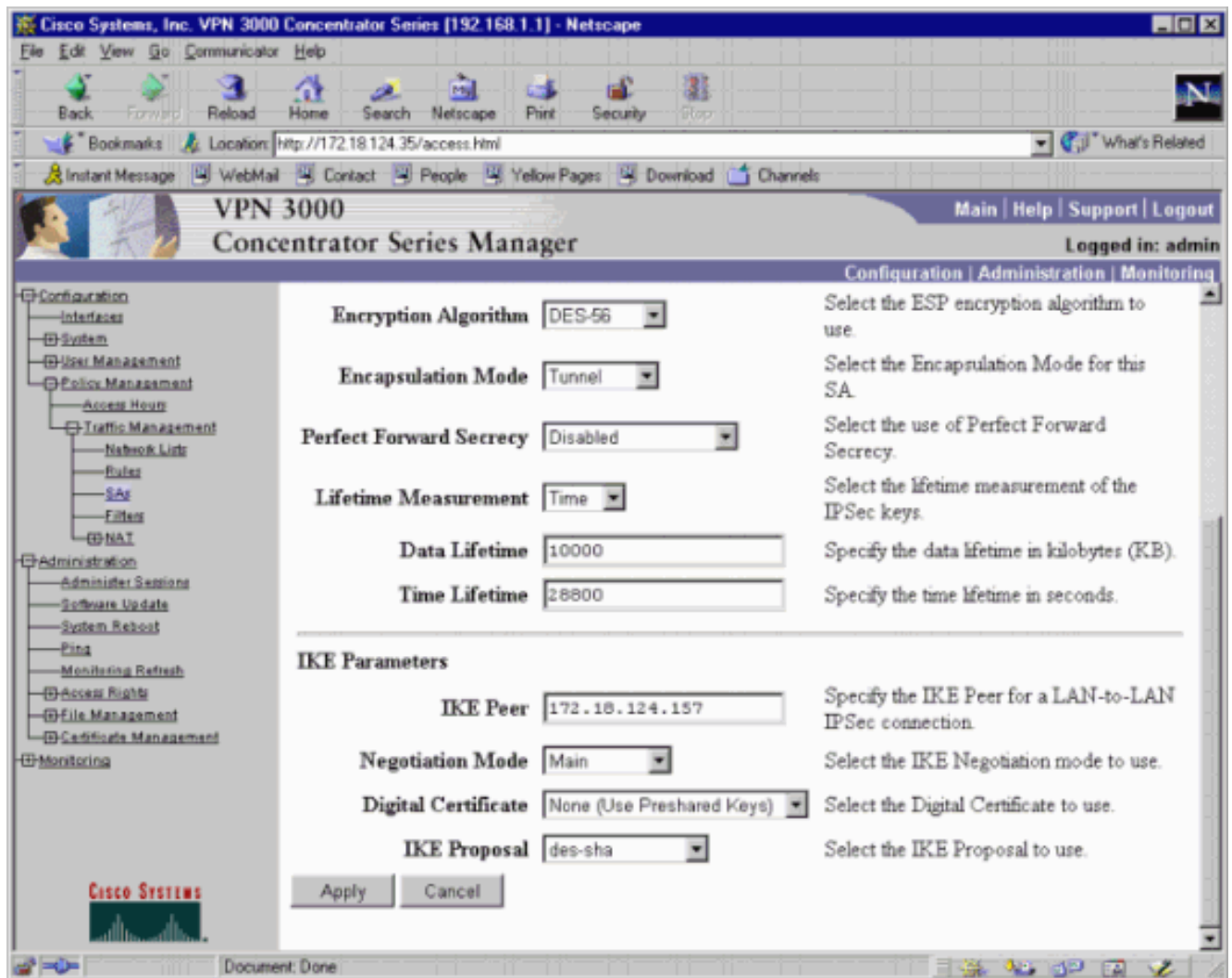
Lifetime Measurement Select the lifetime measurement of the IPSec keys.

Data Lifetime Specify the data lifetime in kilobytes (KB).

Time Lifetime Specify the time lifetime in seconds.

CISCO SYSTEMS

Document: Done

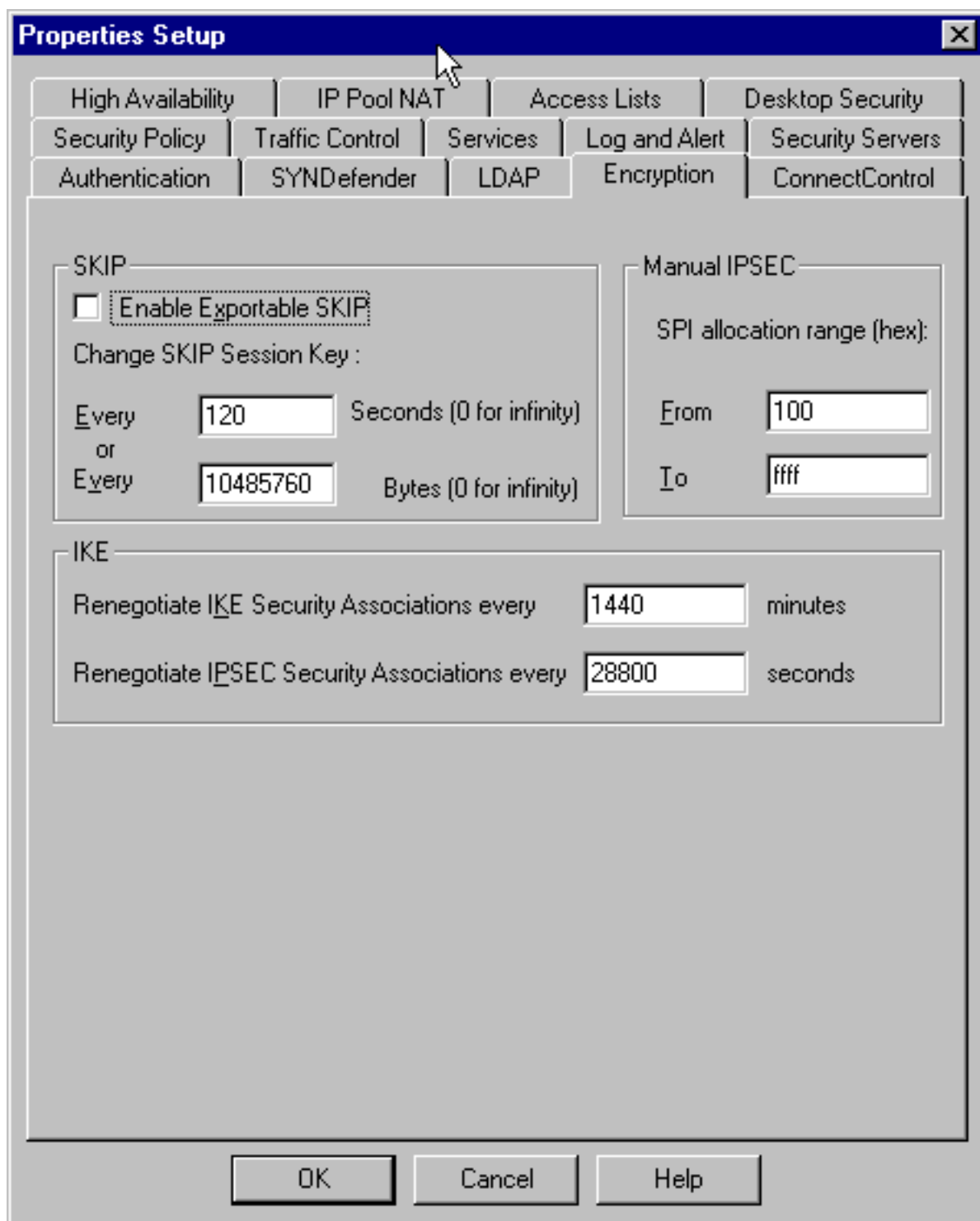


5. 設定を保存します。

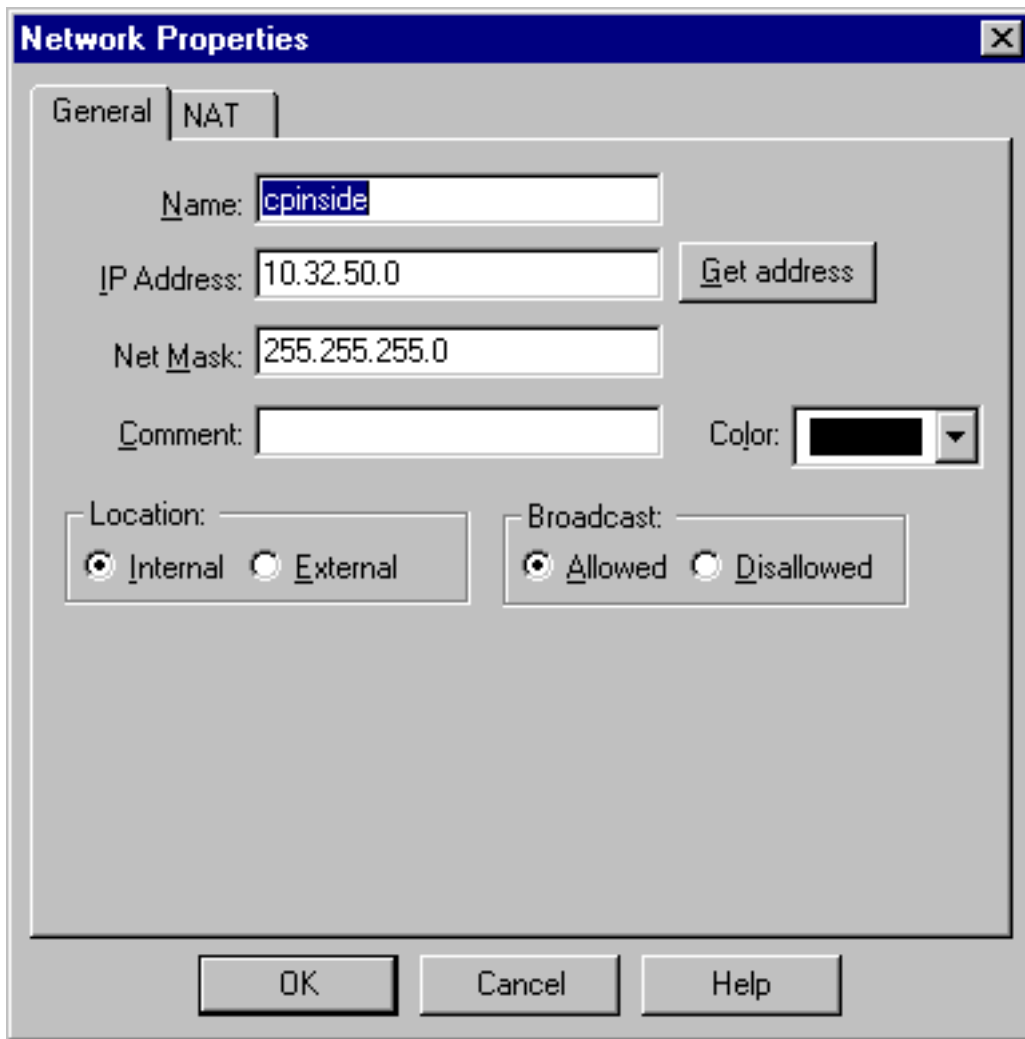
[Checkpoint 4.1 Firewallの設定](#)

Checkpoint 4.1 Firewall を設定するには、次の手順を実行します。

1. IKEとIPsecのデフォルトライフタイムはベンダーによって異なるため、[Properties] > [Encryption]を選択して、CheckpointのライフタイムをVPNコンセントレータのデフォルトと一致するように設定します。VPNコンセントレータのデフォルトIKEライフタイムは86400秒 (1440分) です。VPNコンセントレータのデフォルトIPsecライフタイムは28800秒です。



2. [Manage] > [Network objects] > [New] (または [Edit]) > [Network] の順に選択し、Checkpoint の背後にある内部 (「cpinside」) ネットワークのオブジェクトを設定します。これは、VPNコンセントレータの「リモートネットワーク」と一致している必要があります



3. [Manage] > [Network objects] > [Edit]を選択して、VPNコンソントレータのピアパラメータに含まれるゲートウェイ (「RTPCPVPN」 チェックポイント) エンドポイントのオブジェクトを編集します。Locationの下で Internal を選択します。Type で Gateway を選択します。 [Modules Installed]で、 [VPN-1 & FireWall-1]および[Management Station]にチェックマー

Workstation Properties

General | Interfaces | SNMP | NAT | Certificates | VPN | Authen

Name:

IP Address:

Comment:

Location: Internal External

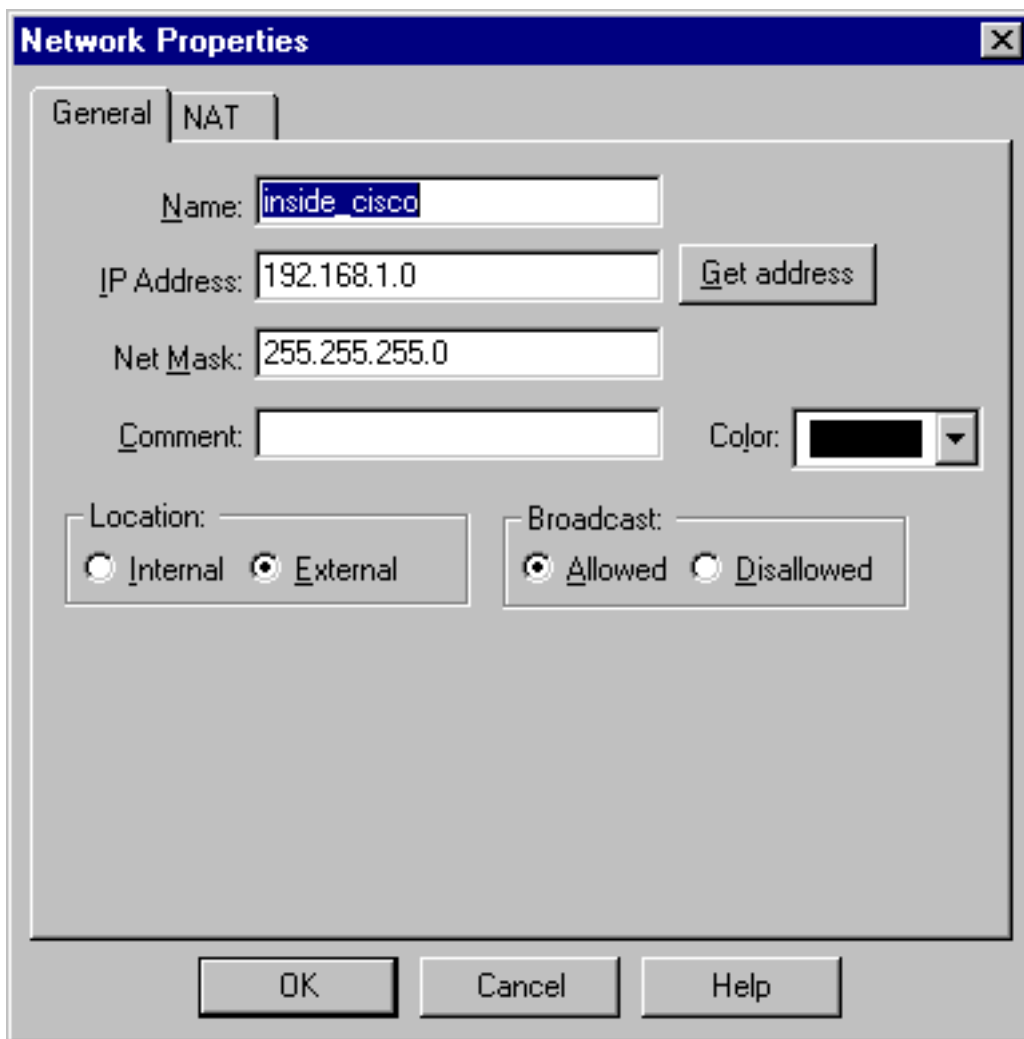
Type: Host Gateway

Modules Installed

<input checked="" type="checkbox"/> VPN-1 & FireWall-1	Version: <input type="text" value="4.1"/>	<input type="button" value="Get"/>
<input type="checkbox"/> FloodGate-1	Version: <input type="text" value="4.1"/>	
<input type="checkbox"/> Compression	Version: <input type="text" value="4.1"/>	
<input checked="" type="checkbox"/> Management Station	Color: <input type="text" value="Black"/>	

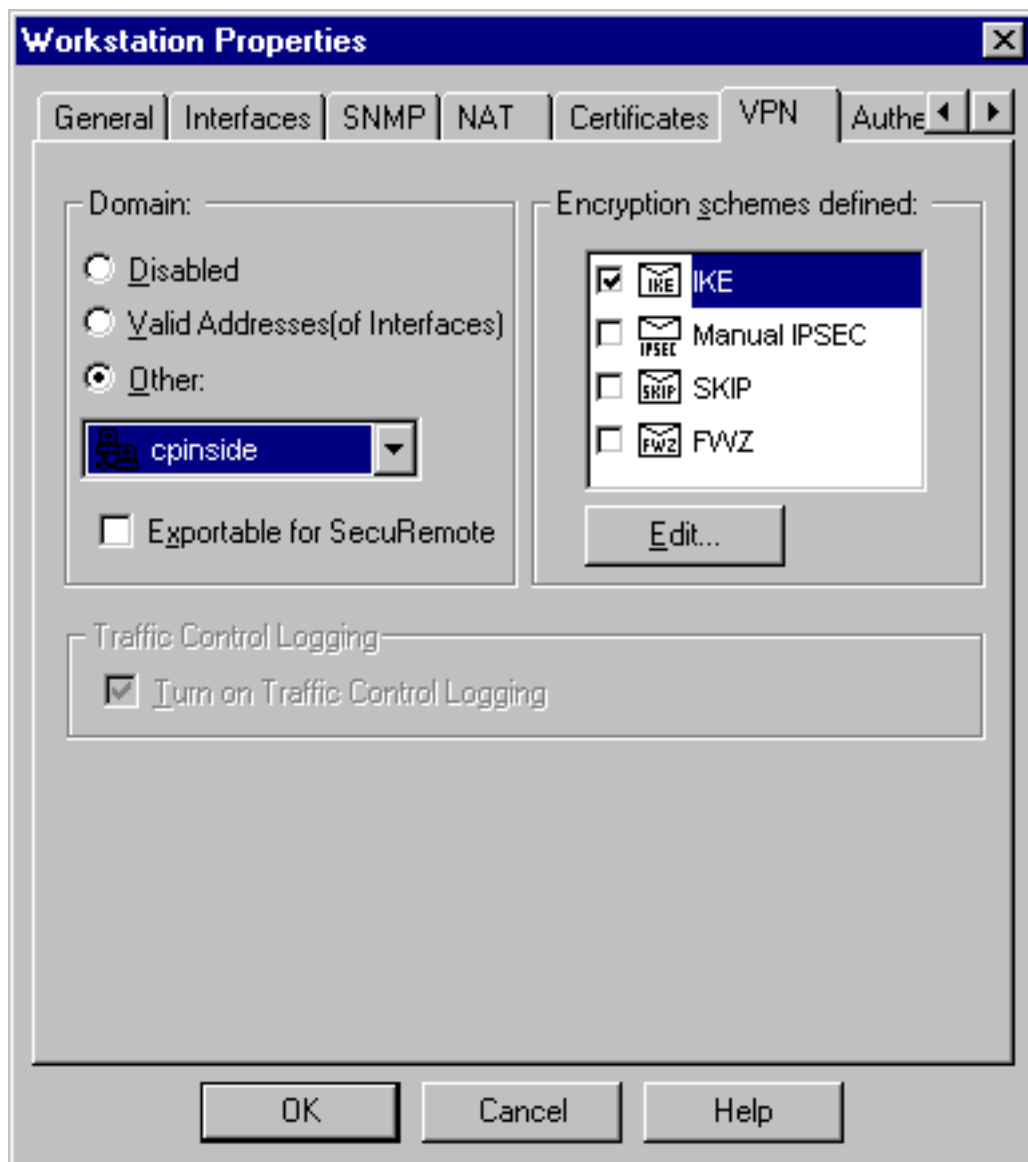
クを付けます。

4. [Manage] > [Network objects] > [New] (または [Edit]) > [Network] の順に選択し、VPN コンセントレータの背後にある外部 (「inside_cisco」) ネットワークのオブジェクトを設定します。これは、VPN コンセントレータの「ローカル」ネットワークと一致している必要があ

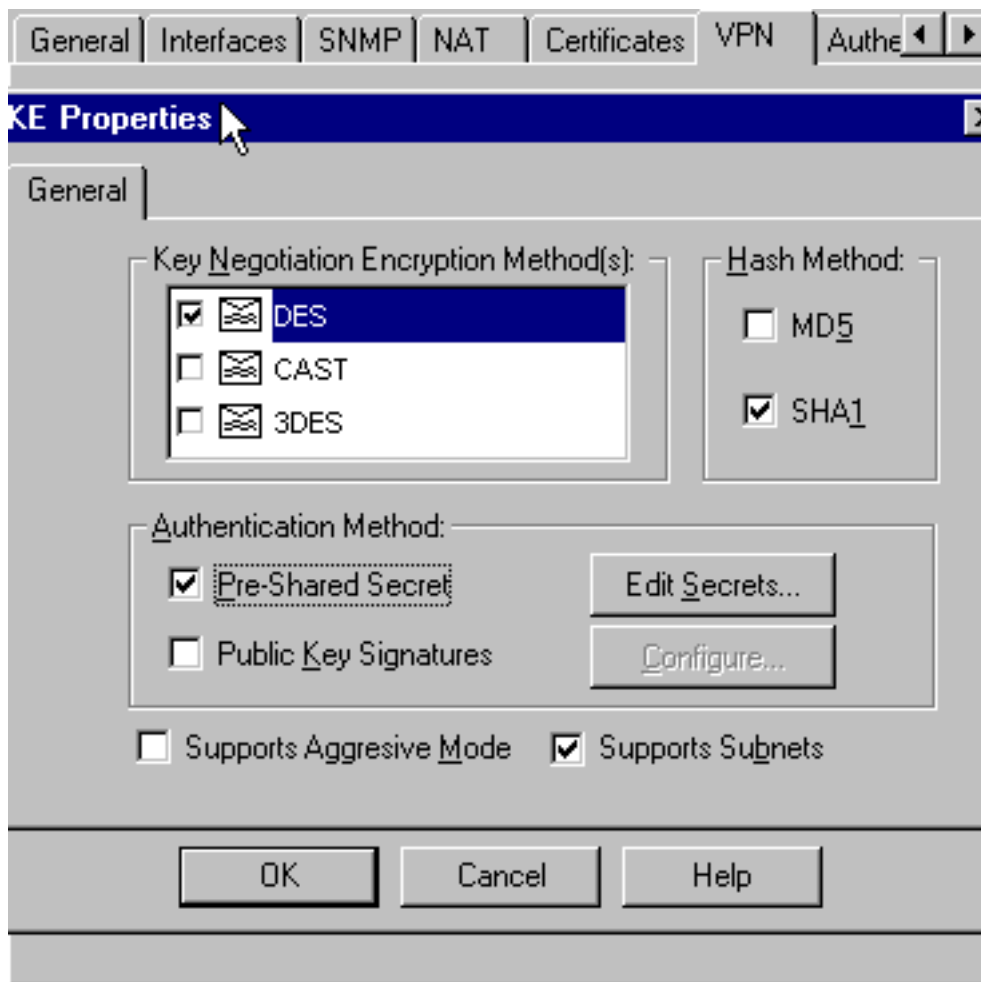


ります。

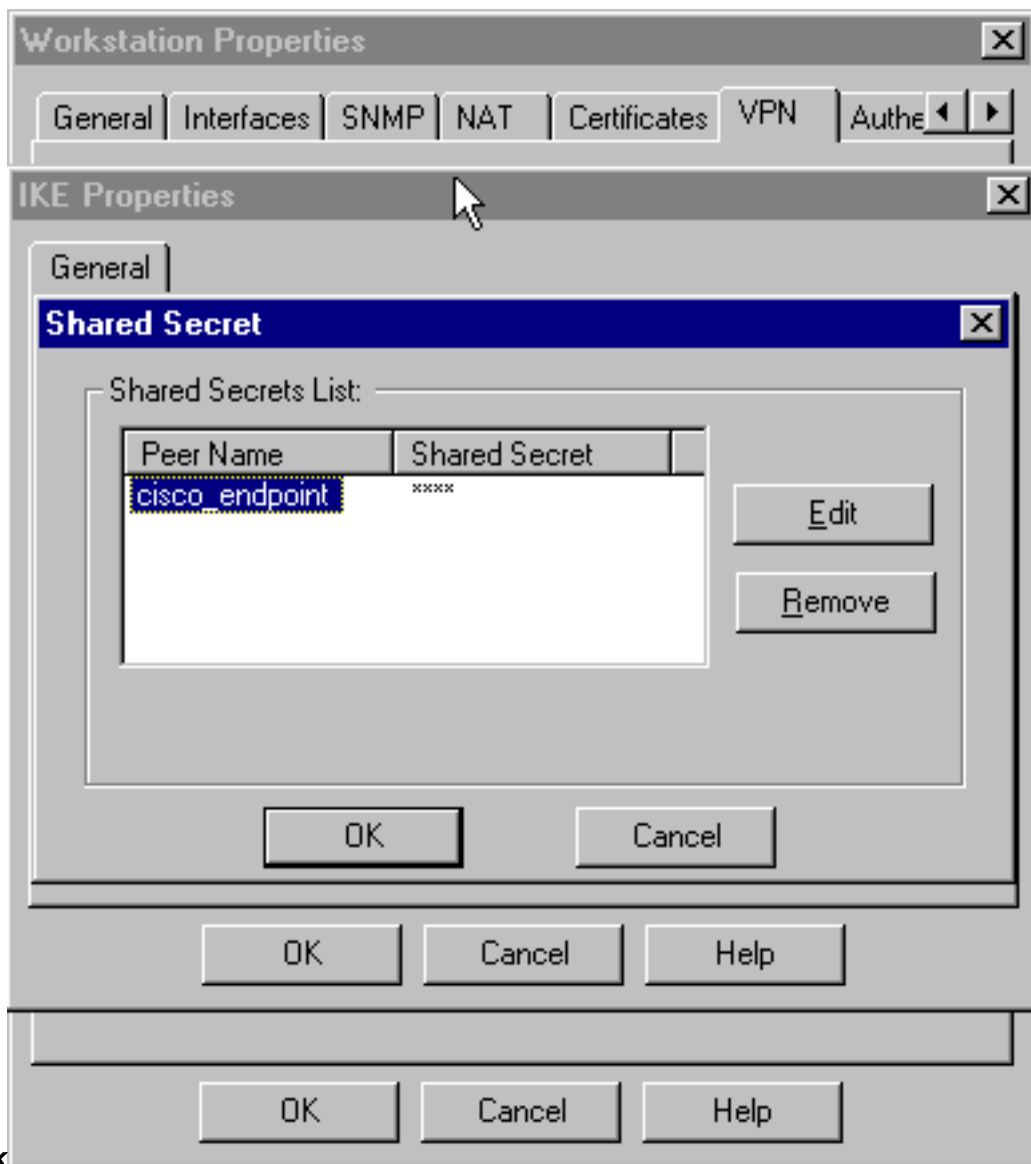
5. [Manage] > [Network objects] > [New] > [Workstation] の順に選択し、外部 (「 cisco_endpoint」) VPN コンセントレータ ゲートウェイのオブジェクトを追加します。これはVPNコンセントレータの「パブリック」インターフェイスです。Locationの下で External を選択します。Type で Gateway を選択します。注 : [VPN-1/FireWall-1]チェックボックスは選択しないでください。
6. [Manage] > [Network objects] > [Edit] の順に選択し、Checkpoint ゲートウェイ エンドポイント (「RTPCPVPN」という名前) の [VPN] タブを編集します。[Domain] の下で、[Other] を選択してから、Checkpoint ネットワークの内側 (「cpinside」という名前) をドロップダウンリストから選択します。[Encryption schemes defined] の下で、[IKE] を選択してから [Edit] をクリックします。



7. DES暗号化のIKEプロパティを、VPNコンセントレータのDES-56および暗号化アルゴリズムと一致するように変更します。
8. VPNコンセントレータのSHA/HMAC-160アルゴリズムと一致するように、IKEプロパティをSHA1ハッシングに変更します。[Aggressive Mode] をオフにします。[Supports Subnets] をオンにします。[Authentication Method] の [Pre-Shared Secret] をオンにします。これは、VPNコンセントレータの認証モードである事前共有キーと同じです。

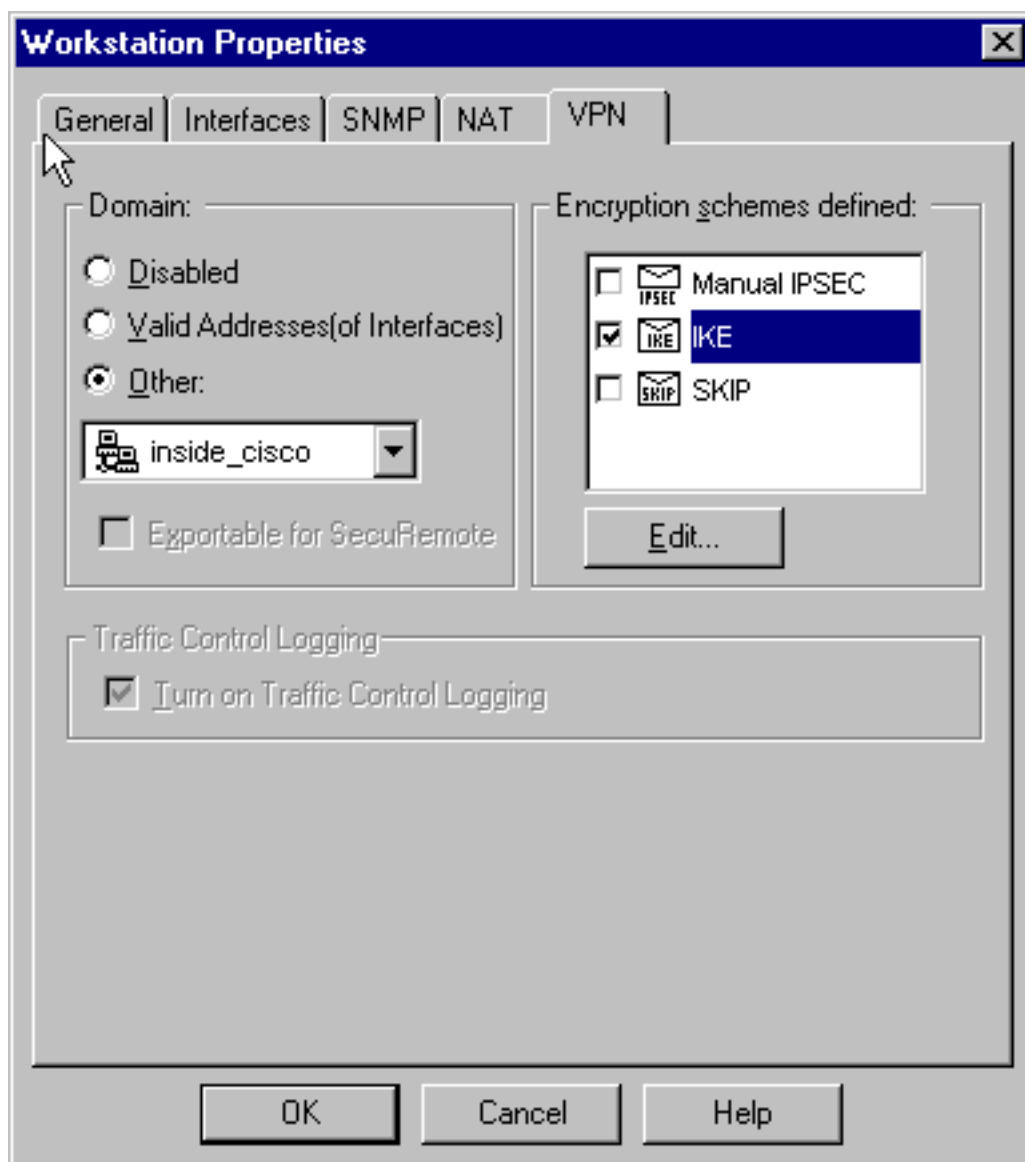


9. [Edit Secrets]をクリックして、事前共有キーを実際のVPNコンソントレータの事前共有キーと一致するように設定します。isakmp key key address address netmask

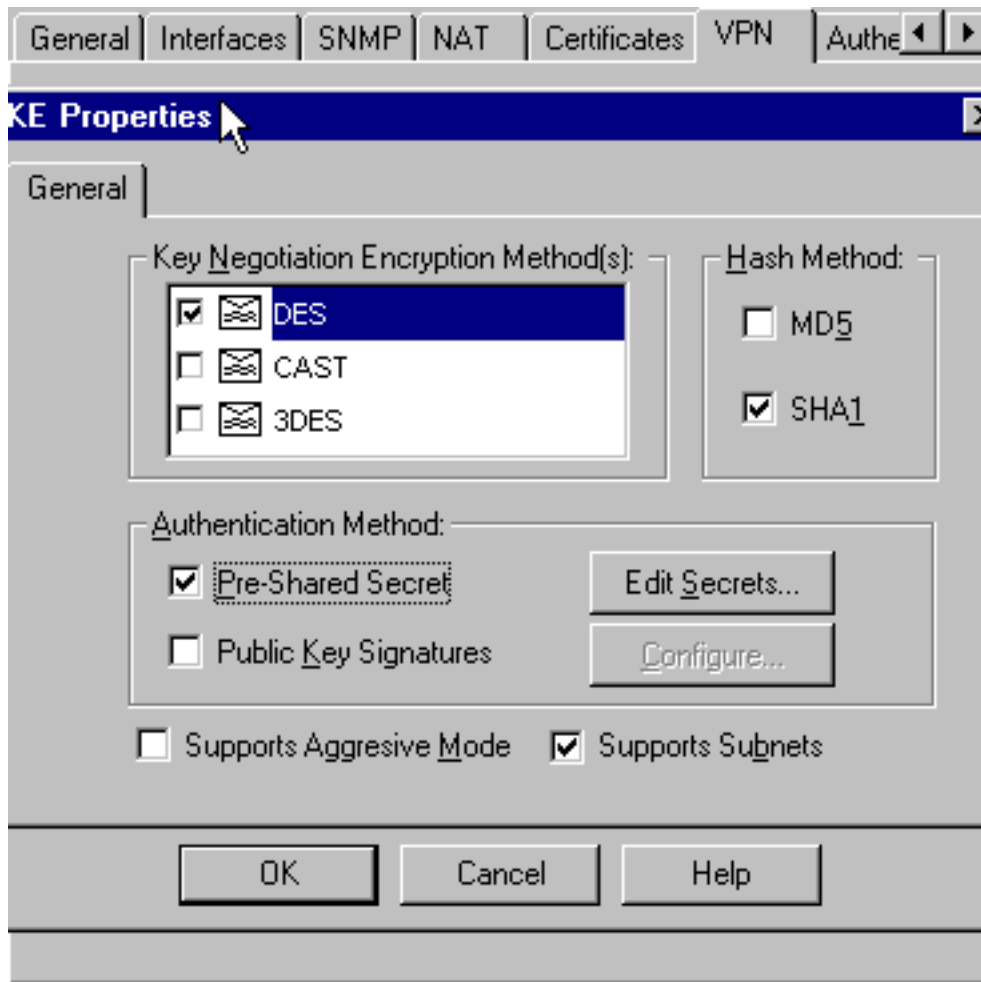


netmask

10. [Manage] > [Network objects] > [Edit] の順に選択し、「cisco_endpoint」の [VPN] タブを編集します。Domain の下で、Other を選択してから Cisco ネットワークの内側（「inside_cisco」という名前）を選択します。[Encryption schemes defined] の下で、[IKE] を選択してから [Edit] をクリックします。

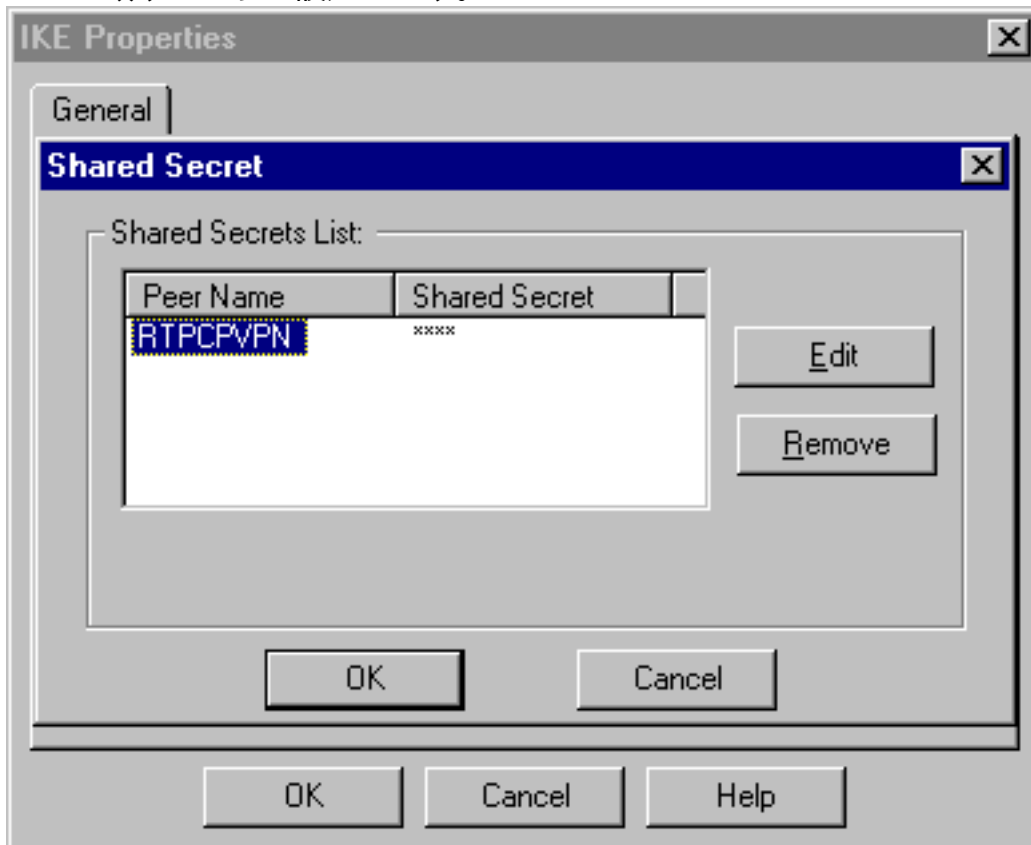


11. VPNコンソントレータのDES-56, Encryption Algorithmと一致するようにIKEプロパティ **DES encryption**を変更します。
12. VPNコンソントレータのSHA/HMAC-160アルゴリズムと一致するように、IKEプロパティをSHA1ハッシングに変更します。次の設定を変更します。Aggressive Mode を選択解除します。[Supports Subnets] をオンにします。[Authentication Method] の [Pre-Shared Secret] をオンにします。これは、事前共有キーのVPNコンソントレータの認証モードと一致しま

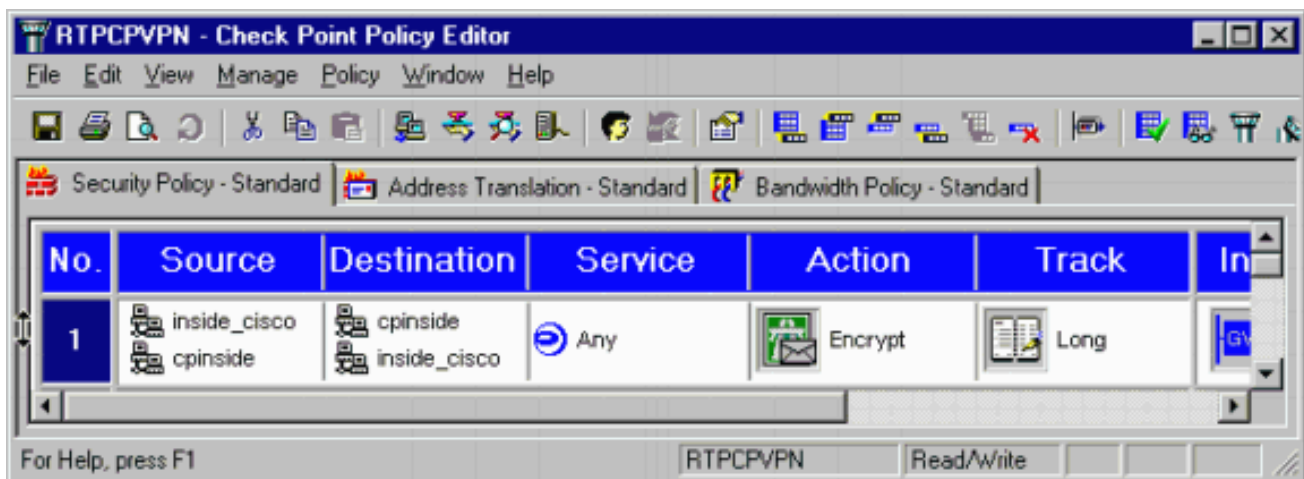


す。

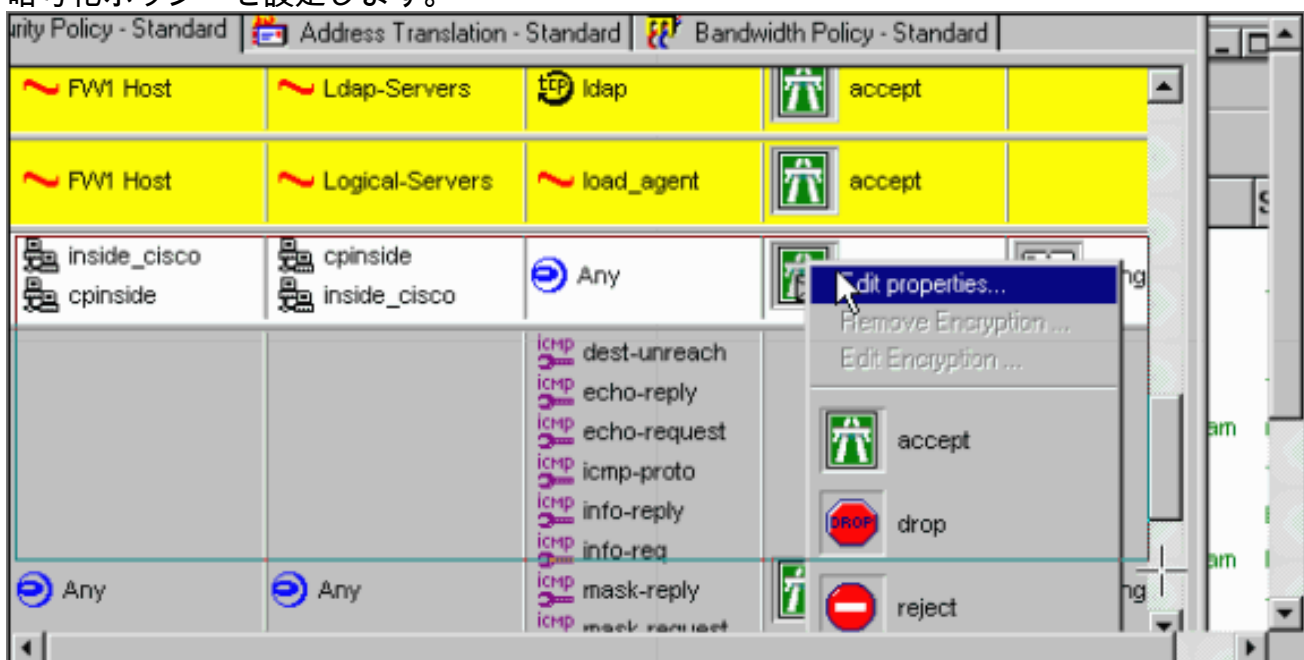
- [Edit Secrets] をクリックして、事前共有キーを実際のVPNコンセントレータの事前共有キーと一致するように設定します。



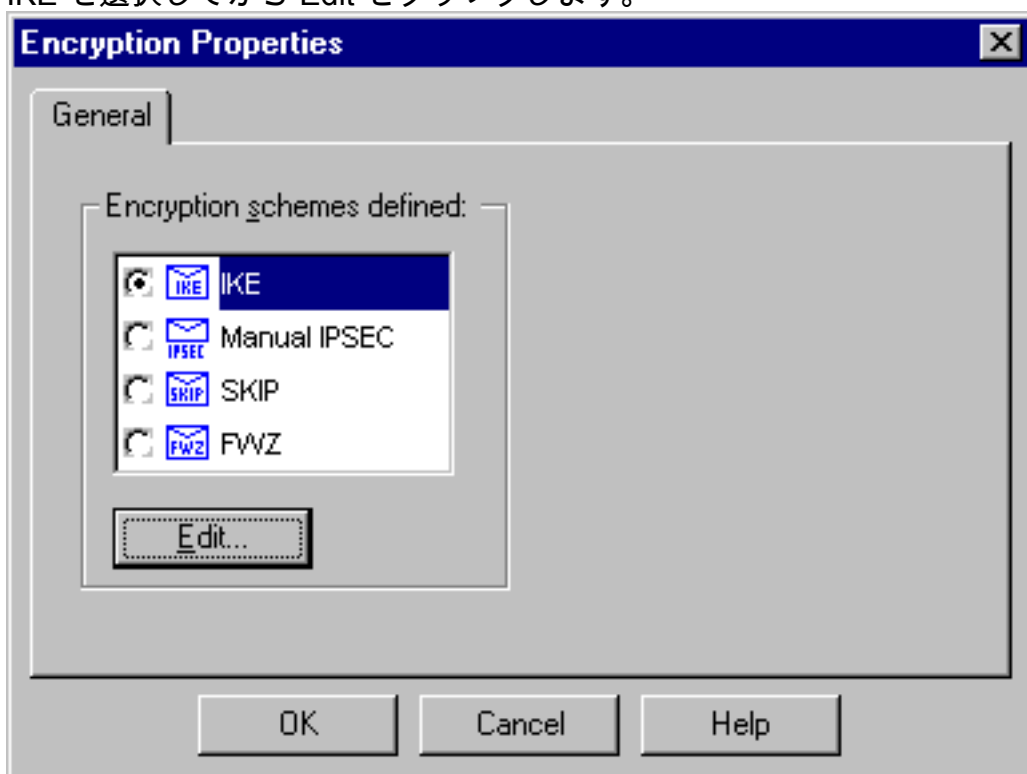
- [Policy Editor] ウィンドウで、Source と Destination の両方に「inside_cisco」と「cpinside」（双方向）を設定したルールを挿入します。Service=Any、Action=Encrypt、および Track=Long を設定します。



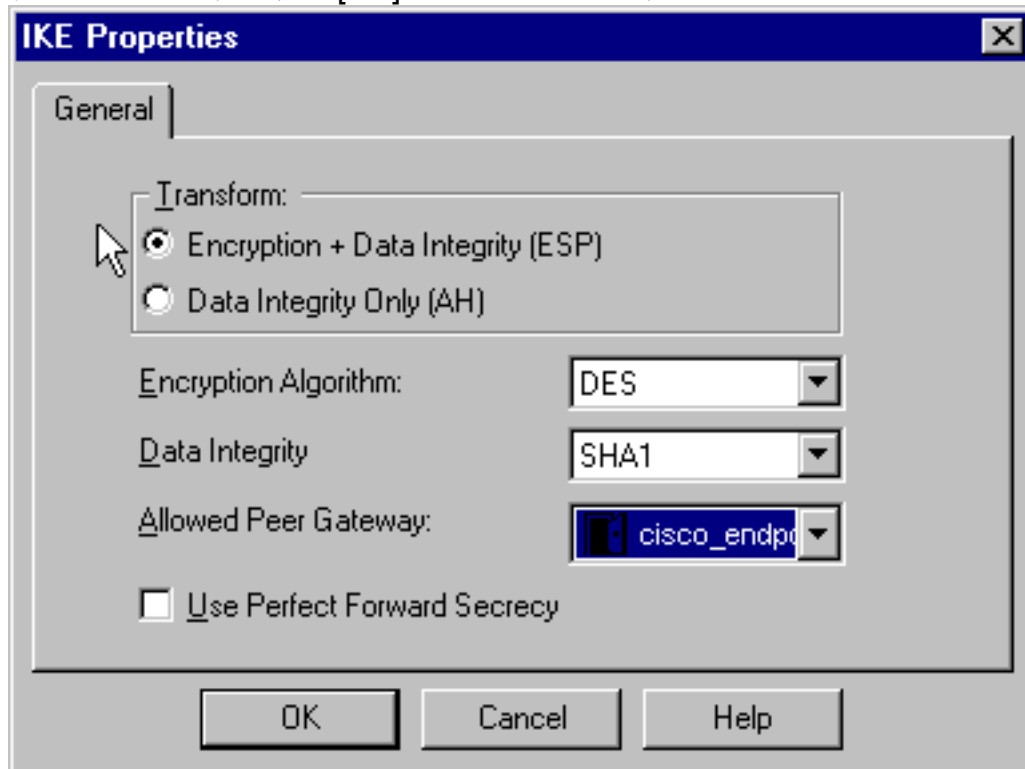
15. [Action] 見出しの下で、緑の [Encrypt] アイコンをクリックし、[Edit properties] を選択して暗号化ポリシーを設定します。



16. IKE を選択してから Edit をクリックします。



17. [IKE Properties]ウィンドウで、これらのプロパティをVPNコンセントレータのIPsecトランスフォームと一致するように変更します。[Transform] の [Encryption + Data Integrity (ESP)] を選択します。Encryption Algorithm は DES に、Data Integrity は SHA1 に、そして Allowed Peer Gateway は外部 Cisco ゲートウェイ (「cisco_endpoint」という名前) に、それぞれなります。[OK] をクリックします。



18. Checkpoint の設定後、[Checkpoint] メニューで [Policy] > [Install] を選択し、変更内容を有効にします。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ネットワーク集約

暗号化ドメイン内の Checkpoint で複数の隣接する内部ネットワークが設定されている場合、このデバイスによってそれらのネットワークが特定のトラフィックに関して自動的に集約されることがあります。VPN コンセントレータが適合するように設定されていない場合、このトンネルに障害が発生する可能性があります。たとえば、10.0.0.0 /24 と 10.0.1.0 /24 の内部ネットワークがトンネルに含まれるように設定されている場合、それらが 10.0.0.0 /23 に集約される可能性があります。

VPN 3000 コンセントレータのデバッグ

VPNコンセントレータのデバッグには、IKE、IKEDBG、IKEDECODE、IPSEC、IPSECDBG、IPSECDECODEが含まれます。デバッグは Configuration > System > Events > Classes で設定し

ます。

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser title is "Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape". The address bar shows "http://172.18.124.35/access.html". The page header includes "VPN 3000 Concentrator Series Manager" and navigation links for "Main | Help | Support | Logout". The user is logged in as "admin".

The left sidebar contains a tree view of the configuration menu:

- Configuration
 - Interfaces
 - System
 - Server
 - Address Management
 - Tunneling Protocols
 - PPTP
 - L2TP
 - IPSec
 - LAN-to-LAN
 - IKE Proposals
 - IP Routing
 - Management Protocols
 - Events
 - General
 - FTP Backup
 - Classes
 - Trap Destinations
 - Syslog Servers
 - SMTP Servers
 - Email Recipients
 - General
 - User Management
 - Policy Management
 - Access Hours
 - Traffic Management
 - Network Lists

The main content area is titled "Configuration | System | Events | Classes" and includes a "Save" button. It contains the following text:

This section lets you configure special handling of specific event classes.

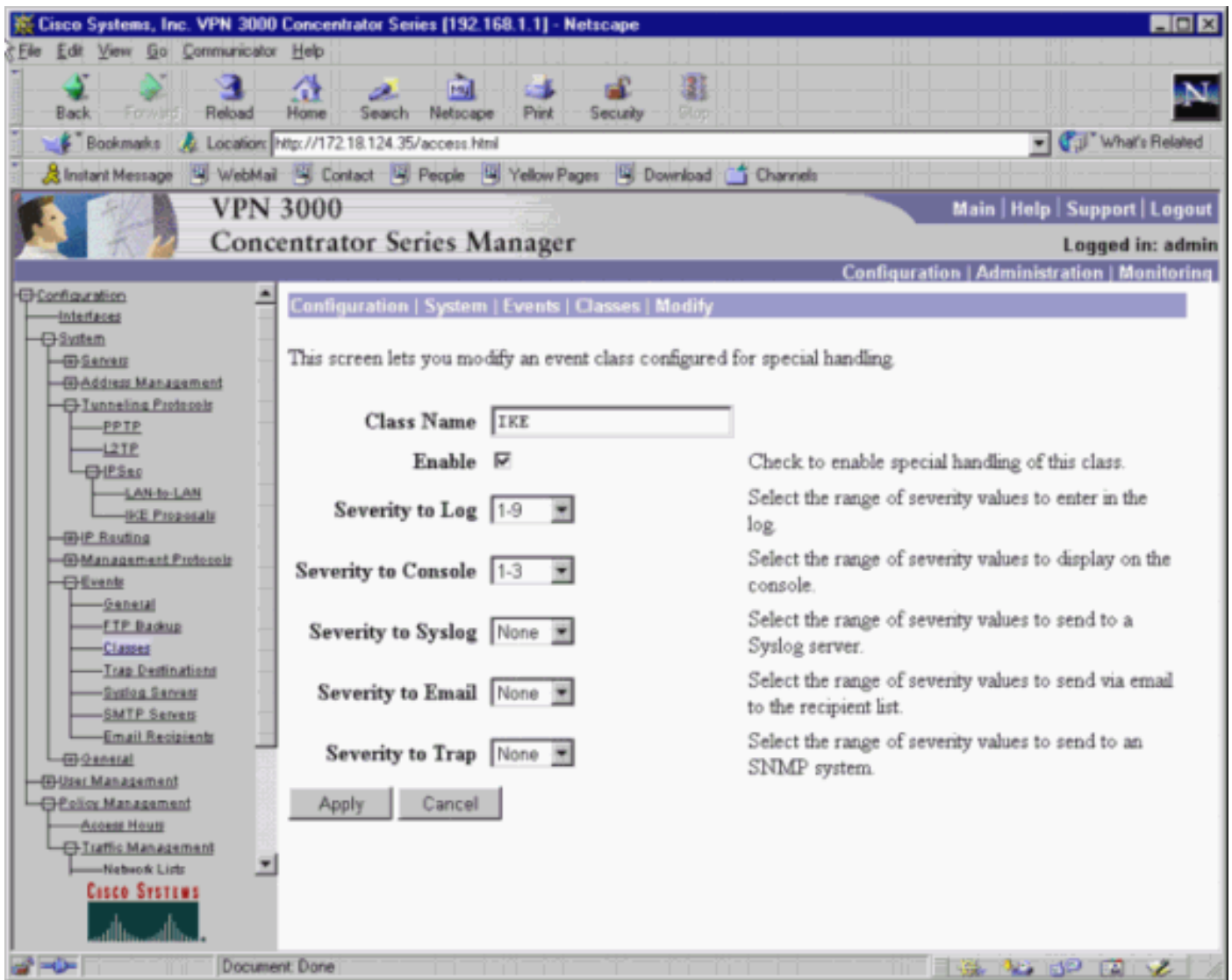
Click the **Add** button to add an event class, or select an event class and click **Modify** or **Delete**.

[Click here to configure general event parameters.](#)

The "Configured Event Classes" section features a list box with the following items:

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

To the right of the list box are three buttons: "Add", "Modify", and "Delete".



デバッグは Monitoring > Event log > Get Log で表示できます。

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser title is "Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Microsoft Internet Explorer". The address bar shows "http://172.18.124.35/access.html". The page title is "VPN 3000 Concentrator Series Manager". The user is logged in as "admin". The navigation menu includes "Main | Help | Support | Logout" and "Configuration | Administration | Monitoring". The left sidebar shows a tree view with "Monitoring" selected. The main content area is titled "Monitoring | Event Log". It includes "Select Filter Options" with "Event Class" set to "AUTH", "Severities" set to "ALL", "Client IP Address" set to "0.0.0.0", and "Events/Page" set to "100". The "Direction" is "Oldest to Newest". There are buttons for "Get Log", "Save Log", and "Clear Log". Below the filters, an event log entry is displayed:

```

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

```

[Monitoring] > [Sessions]を選択して、LAN-to-LANトンネルトラフィックを監視します。

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser title is "Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Microsoft Internet Explorer". The address bar shows "http://172.18.124.35/access.html". The page title is "VPN 3000 Concentrator Series Manager". The user is logged in as "admin". The navigation menu includes "Main | Help | Support | Logout" and "Configuration | Administration | Monitoring". The left sidebar shows a tree view with "Sessions" selected. The main content area displays session statistics and details.

LAN-to-LAN Sessions	Remote Access Sessions	Management Sessions	Active Sessions	Concurrent Sessions	Sessions Limit	Cumulative Sessions
1	0	1	2	3	10000	17

LAN-to-LAN Sessions [[Remote Access Sessions](#) | [Management Sessions](#)]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
to_checkpoint	172.18.124.157	IPSec/LAN-to-LAN	DES-56	Feb 13 14:21:31	0:44:25	1664	1664

Remote Access Sessions [[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
----------	-------------------	---------------------	----------	------------	------------	----------	----------	----------

[Administration] > [Administer Sessions] > [LAN-to-LAN sessions] > [Actions - Logout]の順に選択し、トンネルをクリアします。

Checkpoint 4.1 Firewall のデバッグ

注：これはMicrosoft Windows NTのインストールです。トラッキングは Policy Editor ウィンドウで Long に設定されているため、拒否されたトラフィックがログ ビューアに赤で表示されます。より詳細なデバッグは、次のコマンドで取得できます。

```
C:\WINNT\FW1\4.1\fwstop
```

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

さらに、別のウィンドウで次のコマンドを実行します。

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

チェックポイントでSAをクリアするには、次のコマンドを発行します。

```
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
```

「Are you sure ?」というプロンプトには「yes」とプロンプトで表示されない場合があります。

debug 出力例

Cisco VPN 3000 コンセントレータ

```
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 length : 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: rcv 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 length : 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

[関連情報](#)

- [IPSec ネゴシエーション/IKE プロトコル](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)