Cisco VPN 3000 コンセントレータと Checkpoint NG Firewall 間のIPSec トンネル設定

内容

概要

このドキュメントでは、2 つのプライベート ネットワーク間で通信するために事前共有キーを使用して IPSec トンネルを設定する方法について説明します。この例では、通信するネットワークは、Cisco VPN 3000 コンセントレータ内部の 192.168.10.x プライベート ネットワークと Checkpoint Next Generation（NG）ファイアウォール内部の 10.32.x.x プライベート ネットワークです。

前提条件

要件

- VPNコンセントレータ内部およびCheckpoint NG内部からインターネット(ここでは172.18.124.xネットワークで表される)へのトラフィックは、この設定を開始する前にフローする必要があります。
- ユーザはIPSecネゴシエーションに精通している必要があります。このプロセスは、2つのインターネットキー交換(IKE)フェーズを含む5つのステップに分けることができます。対象ト

ラフィックによって IPSec トンネルが開始されます。IPsec ピアの間を転送されるトラフィックは、対象トラフィックとみなされます。IKE フェーズ 1 では、IPSec ピア同士が、IKE Security Association (SA; セキュリティ結合) ポリシーについてネゴシエートします。ピアが認証されると、Internet Security Association and Key Management Protocol(ISAKMP)を使用してセキュアトンネルが作成されます。IKEフェーズ2では、IPSecピアは、IPSec SAトランスフォームをネゴシエートするために、認証された安全なトンネルを使用します。共有ポリシーのネゴシエーションによって、IPsec トンネルの確立方法が決まります。IPSecトンネルが作成され、IPSecトランスフォームセットで設定されたIPSecパラメータに基づいて、IPSecピア間でデータが転送されます。IPsec SA が削除されるか、そのライフタイムの有効期限が切れると、IPsec トンネルは終了します。

使用するコンポーネント

この設定は、次のバージョンのソフトウェアとハードウェアを使用して作成およびテストされています。

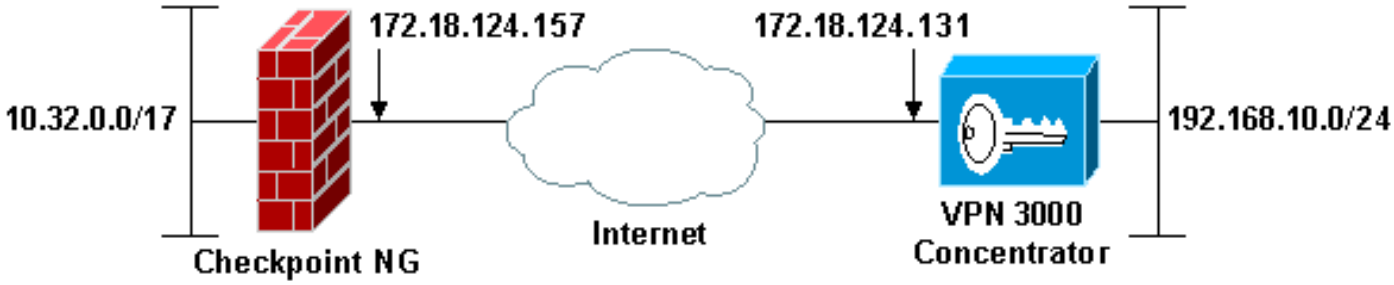
- VPN 3000シリーズコンセントレータ3.5.2
- Checkpoint NG Firewall

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。

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。



注：この設定で使用されるIPアドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。これらはラボ環境で使用された RFC 1918 のアドレスです。

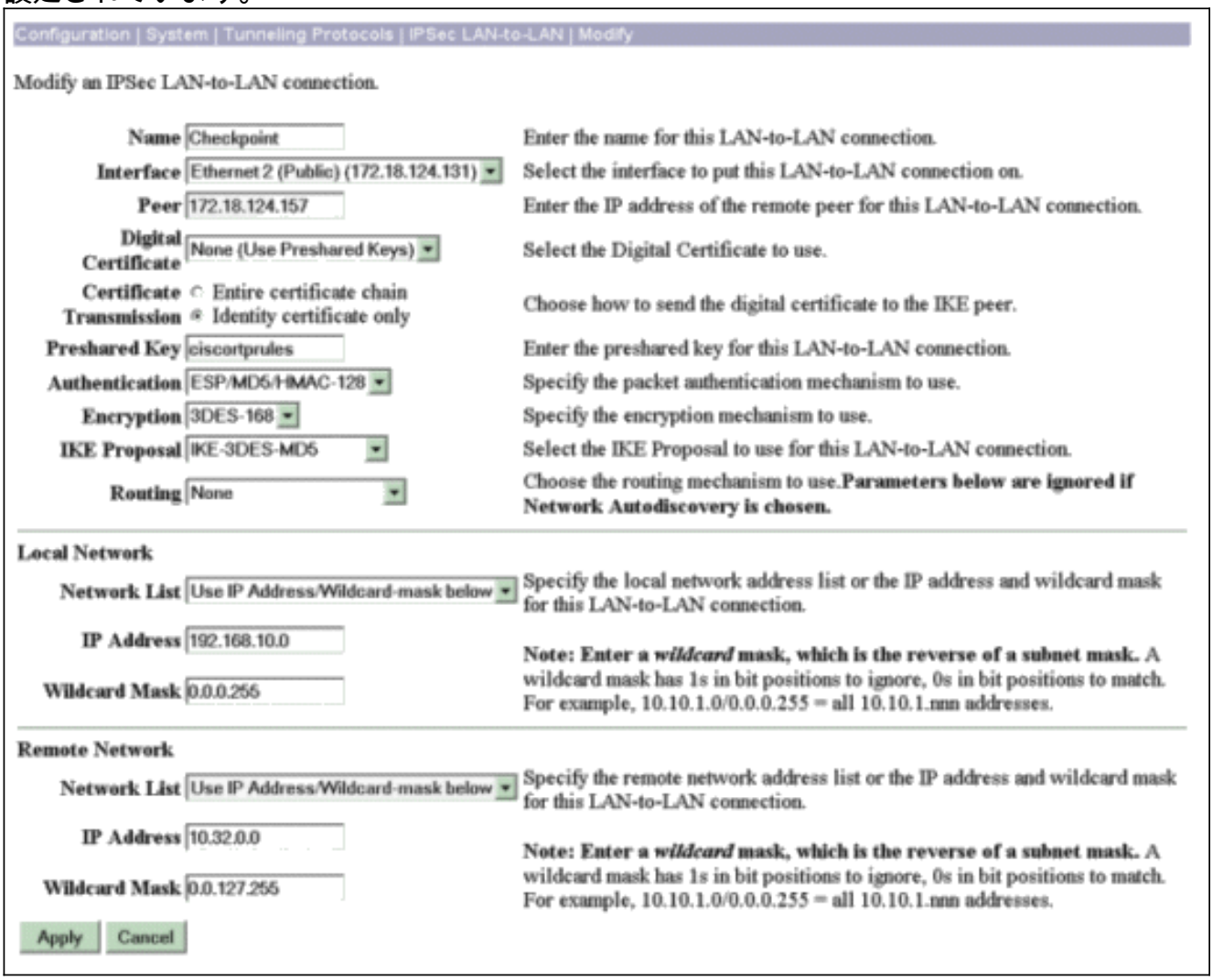
設定

VPN 3000 コンセントレータの設定

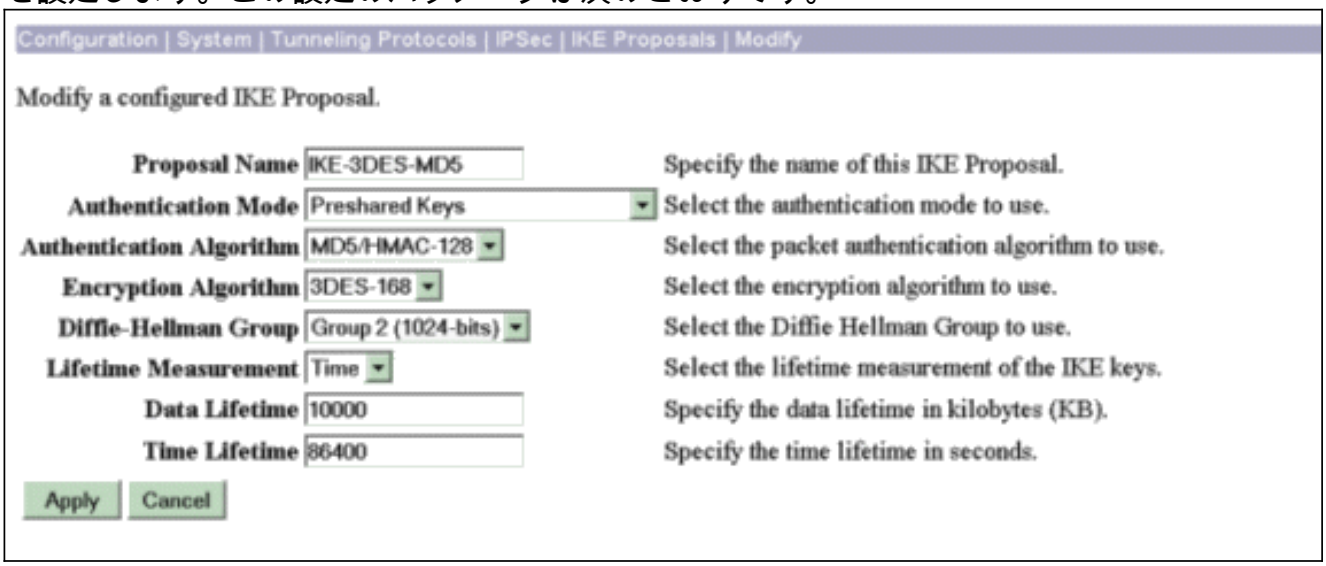
VPN 3000コンセントレータを設定するには、次の手順を実行します。

1. **[Configuration] > [System] > [Tunneling Protocols] > [IPSec LAN-to-LAN]に移動**して、LAN-to-LANセッションを設定します。認証およびIKEアルゴリズム、事前共有キー、ピアIPアドレス、ローカルおよびリモートネットワークパラメータのオプションを設定します。[Apply]をクリックします。この設定では、認証はESP-MD5-HMACに設定され、暗号化は3DESに

設定されています。

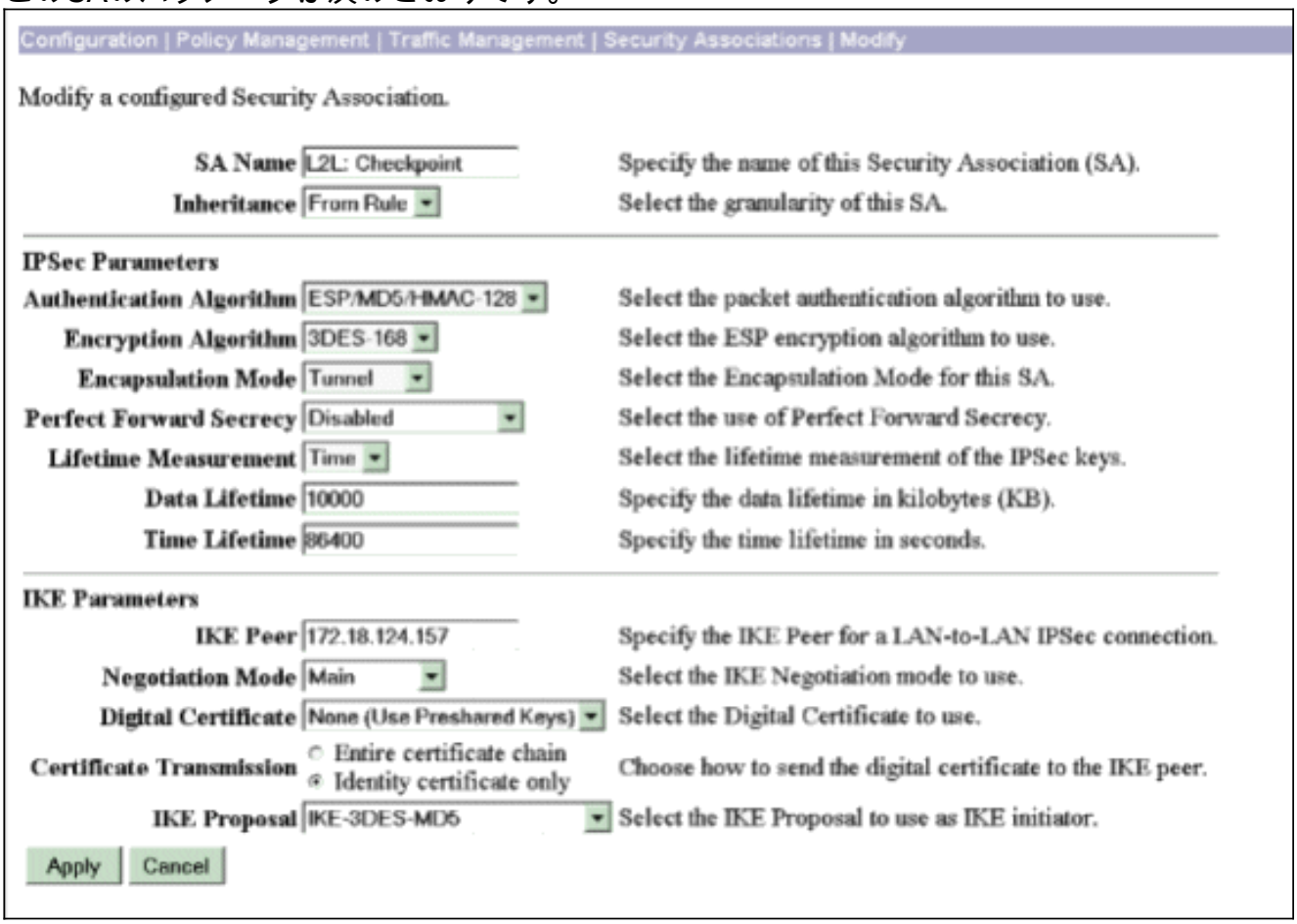


2. Configuration > System > Tunneling Protocols > IPSec > IKE Proposalsの順に選択し、必要なパラメータを設定します。IKEプロポーザルIKE-3DES-MD5を選択し、プロポーザルに対して選択されたパラメータを確認します。[Apply]をクリックして、LAN-to-LANセッションを設定します。この設定のパラメータは次のとおりです。



3. [Configuration] > [Policy Management] > [Traffic Management] > [Security Associations] に移動し、セッション用に作成されたIPSec SAを選択し、LAN-to-LANセッション用に選択されたIPSec SAパラメータを確認します。この設定では、LAN-to-LANセッション名は「Checkpoint」であるため、IPSec SAは自動的に「L2L:チェックポイント。」

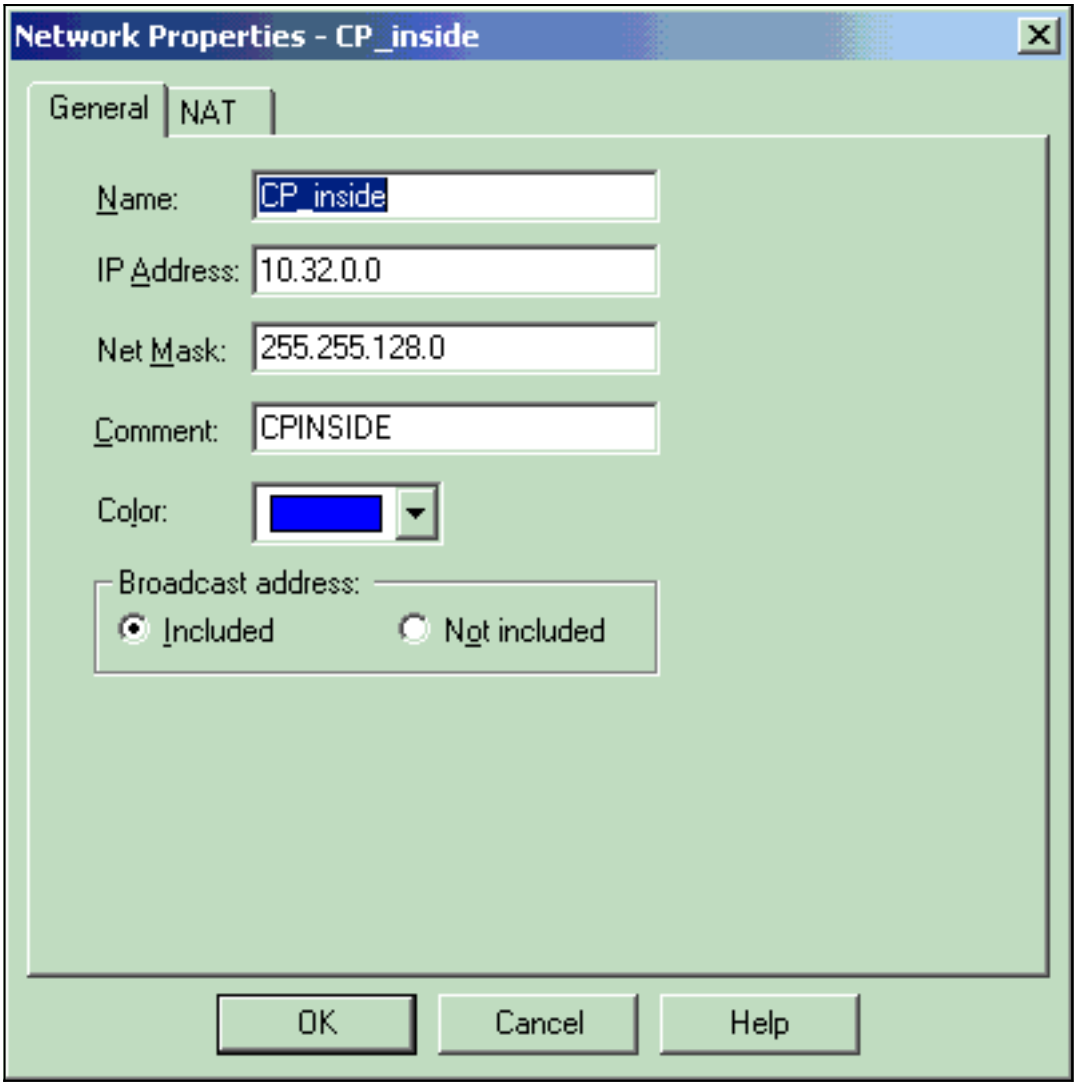
このSAのパラメータは次のとおりです。

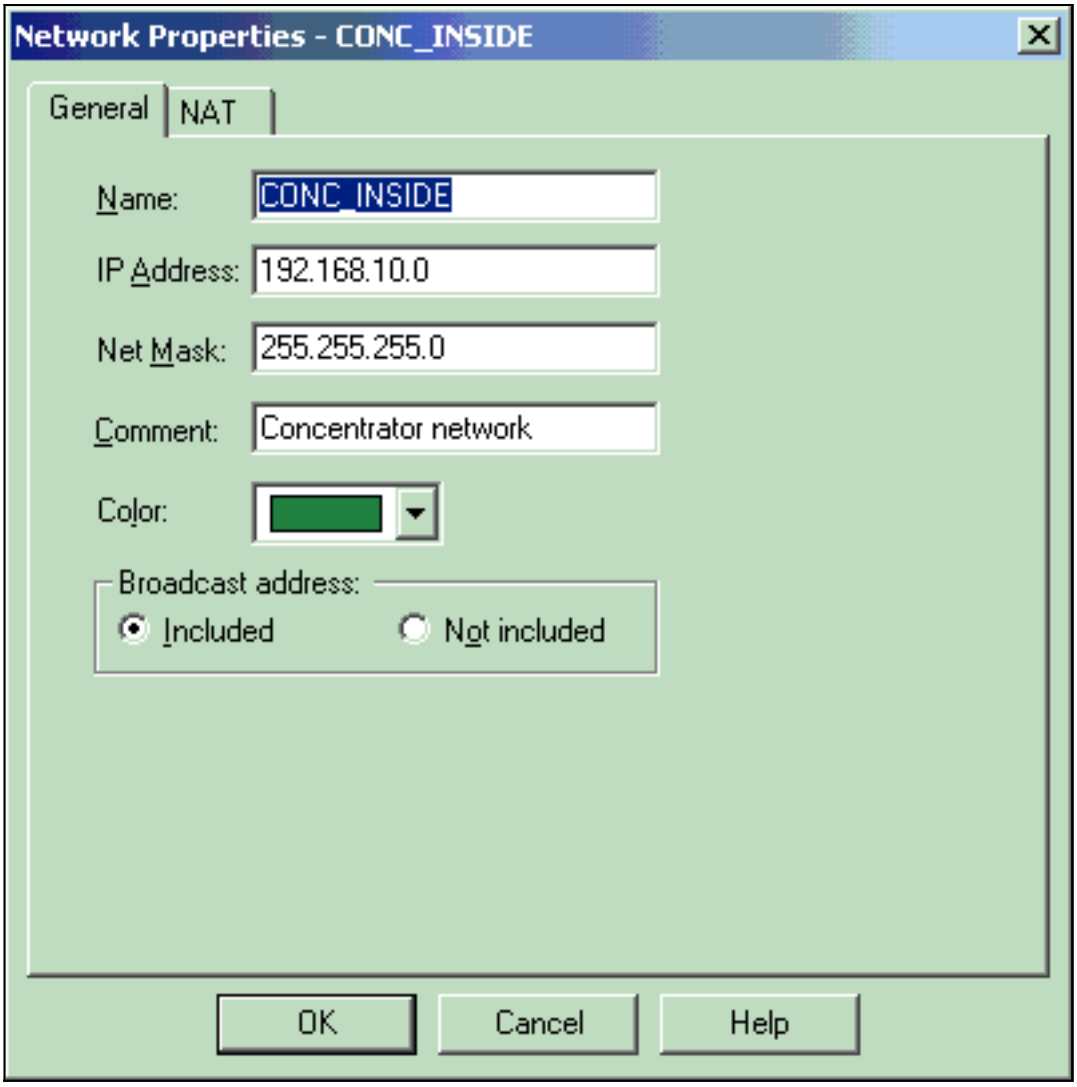


Checkpoint NG の設定

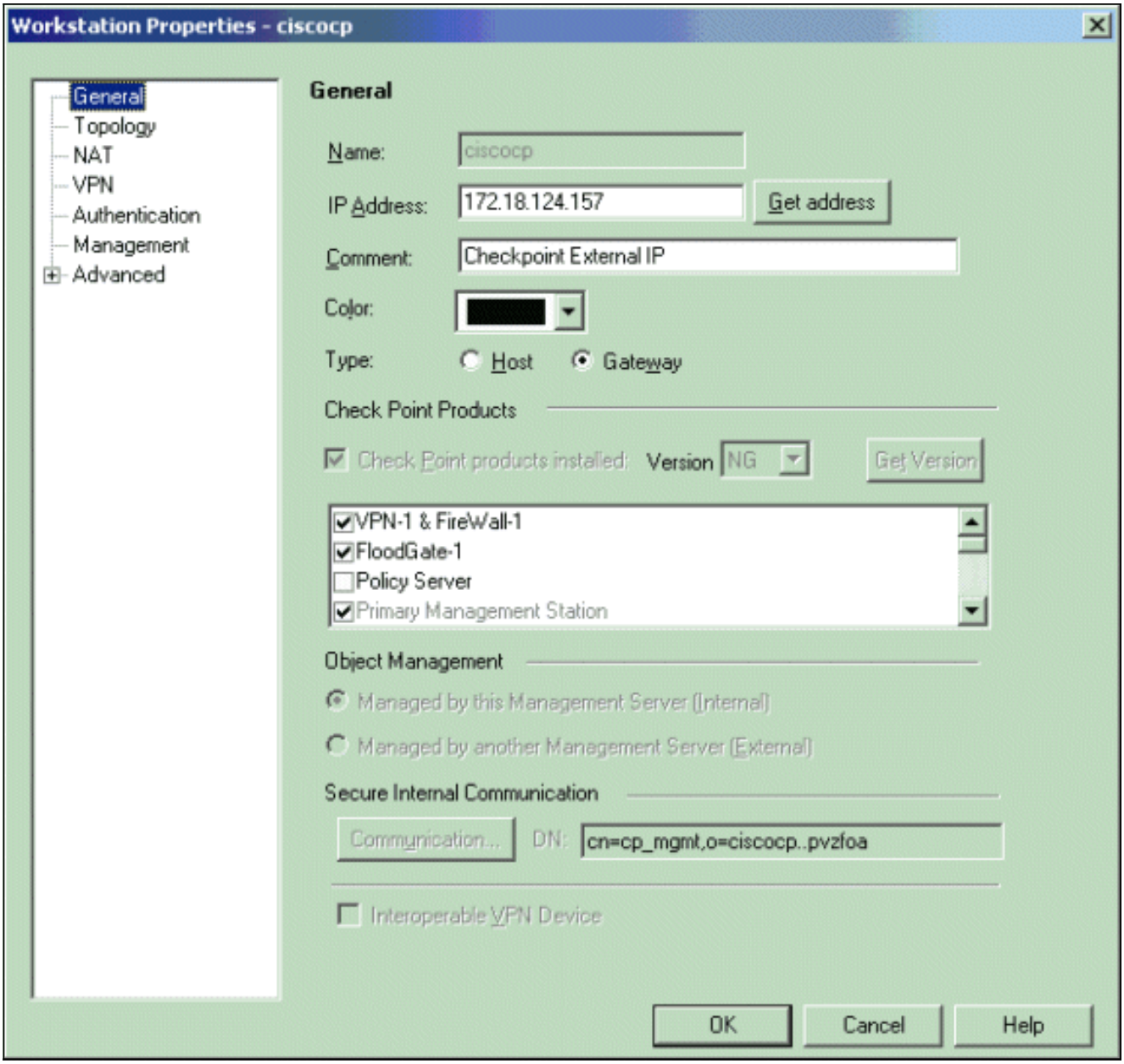
設定するVPN設定に関連するポリシーを作成するために、Checkpoint NGでネットワークオブジェクトとルールが定義されます。このポリシーは、Checkpoint NG Policy Editorとともにインストールされ、設定のCheckpoint NG側を完了します。

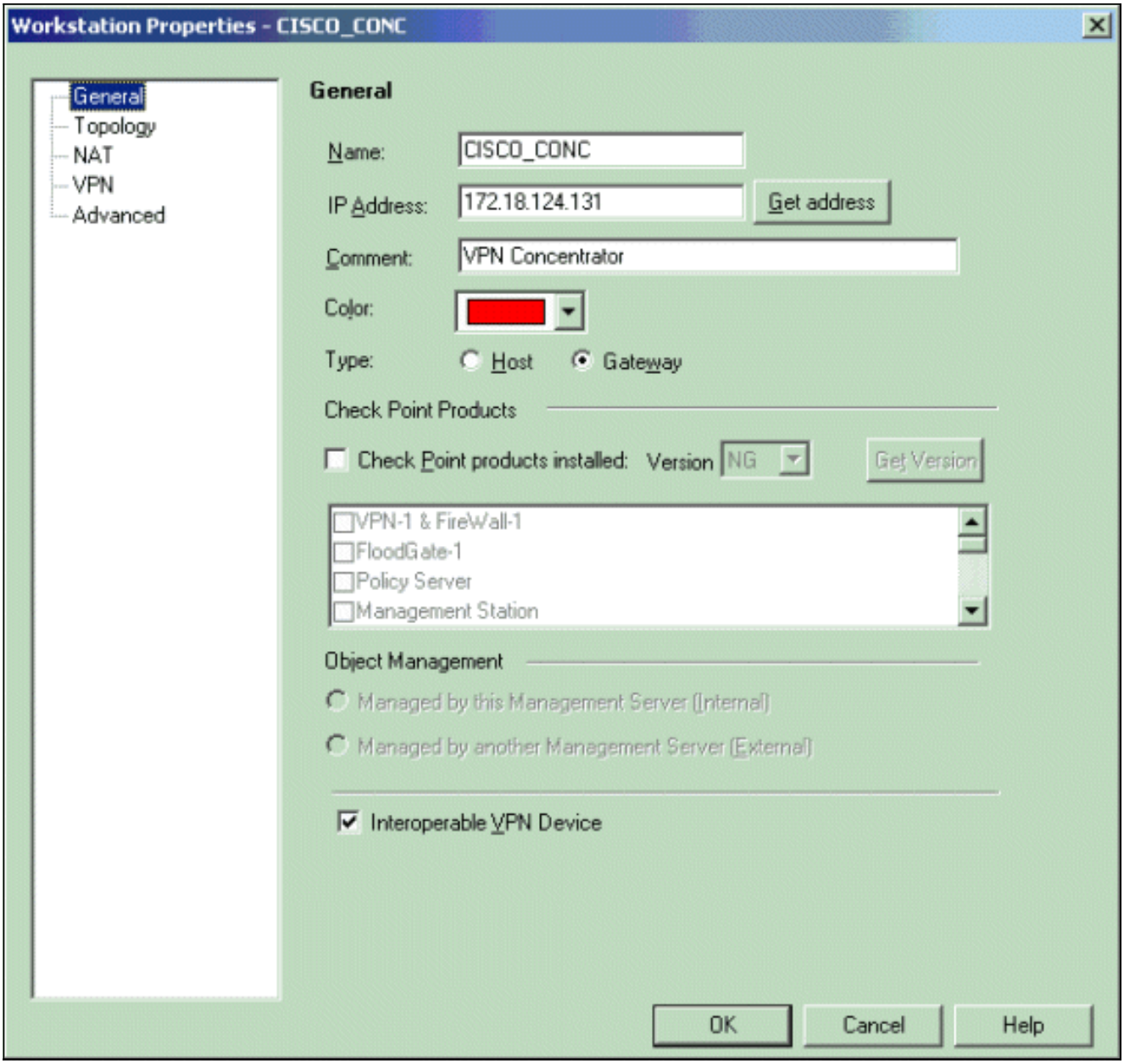
1. 対象トラフィックを暗号化するCheckpoint NGネットワークとVPNコンセントレータネットワークの2つのネットワークオブジェクトを作成します。オブジェクトを作成するには、**[Manage] > [Network Objects]を選択**し、**[New] > [Network]を選択します**。適切なネットワーク情報を入力して、[OK] をクリックします。次の例は、CP_inside（Checkpoint NGの内部ネットワーク）およびCONC_INSIDE（VPNコンセントレータの内部ネットワーク）と呼ばれるネットワークオブジェクトの設定を示しています。


Network Properties - CP_inside
General
NAT
Name:
CP_inside
IP Address:
10.32.0.0
Net Mask:
255.255.128.0
Comment:
CPINSIDE
Color:
Broadcast address:
Included
Not included
OK
Cancel
Help

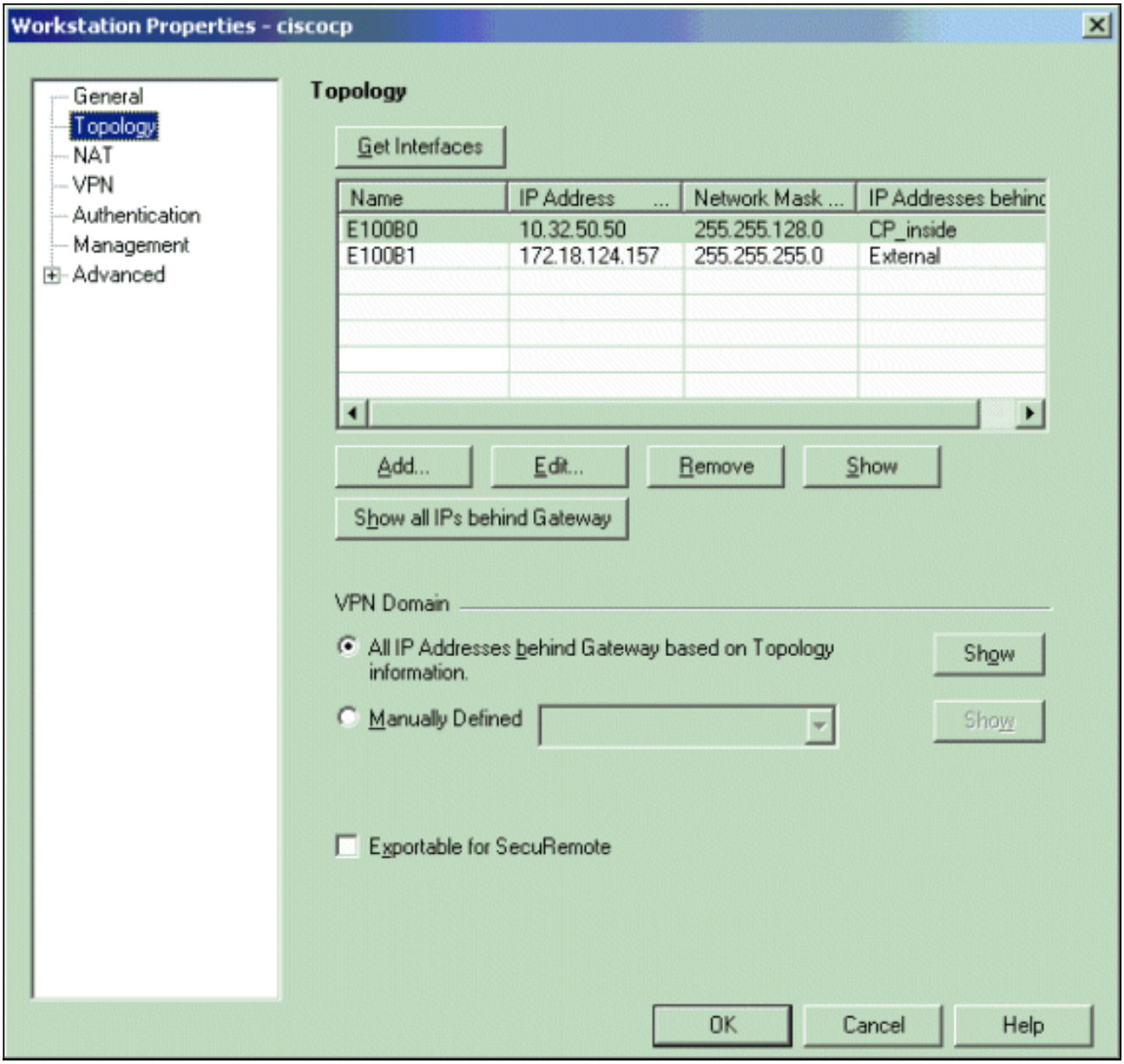


2. VPNデバイス、Checkpoint NG、およびVPNコンセントレータのワークステーションオブジェクトを作成するには、[Manage] > [Network Objects]に移動し、[New] > [Workstation]を選択します。**注：初期**Checkpoint NGセットアップ時に作成されたCheckpoint NGワークステーションオブジェクトを使用できます。ワークステーションをゲートウェイおよび相互運用可能VPNデバイスとして設定するオプションを選択し、[OK]をクリ**ックします**。次の例は、ciscocp(Checkpoint NG)およびCISCO_CONC（VPN 3000コンセントレータ）と呼ばれるオブジェクトのセットアップを示しています。

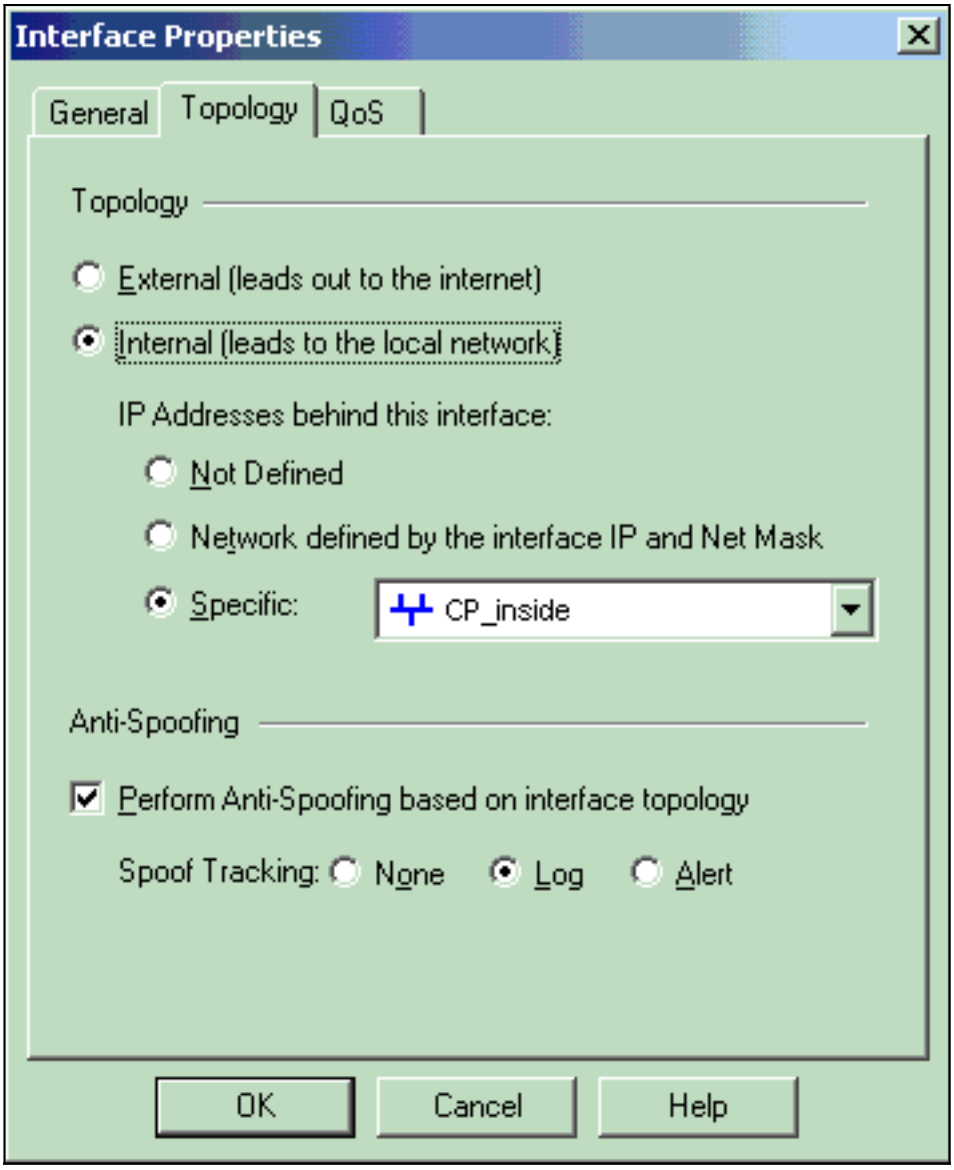

Workstation Properties - ciscocp
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
ciscocp
IP Address:
172.18.124.157
Get address
Comment:
Checkpoint External IP
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
FloodGate-1
Policy Server
Primary Management Station
Object Management
Managed by this Management Server (Internal)
Managed by another Management Server (External)
Secure Internal Communication
Communication...
DN:
cn=cp_mgmt,o=ciscocp..pvzfoa
Interoperable VPN Device
OK
Cancel
Help



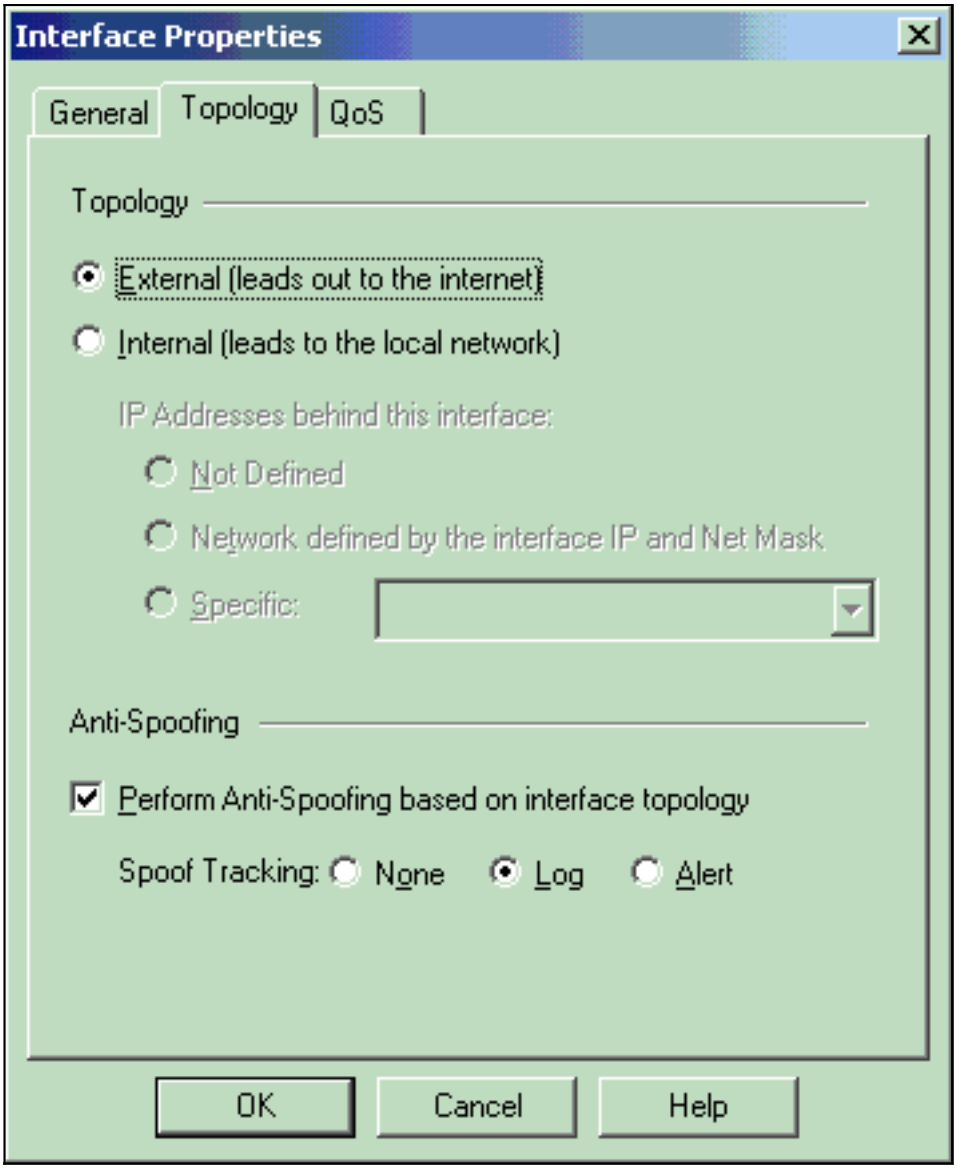
3. [**Manage] > [Network Objects] > [Edit]に移動**して、Checkpoint NGワークステーション（この例ではciscocp）の[Workstation Properties]ウィンドウを開きます。 ウィンドウの左側の選択肢から**[Topology]**を選択し、暗号化するネットワークを選択します。**[Edit]**をクリックして、インターフェイスのプロパティを設定します。この例では、CP_insideはCheckpoint NGの内部ネットワークです。



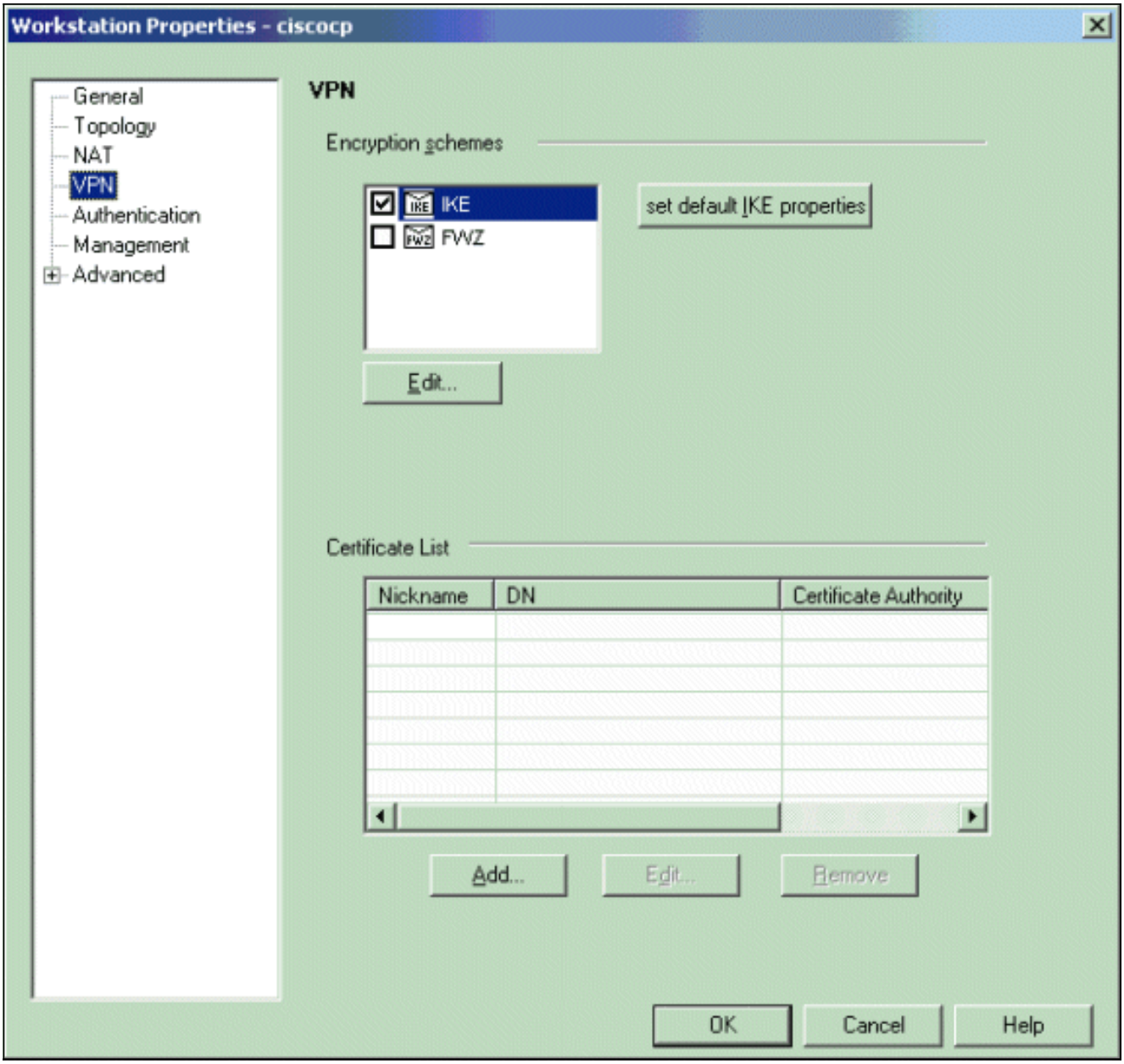
4. [Interface Properties]ウィンドウで、ワークステーションを内部として指定するオプションを選択し、適切なIPアドレスを指定します。[OK] をクリックします。次に示すトポロジ選択では、ワークステーションを内部として指定し、CP_insideインターフェイスの背後にあるIPアドレスを指定します。



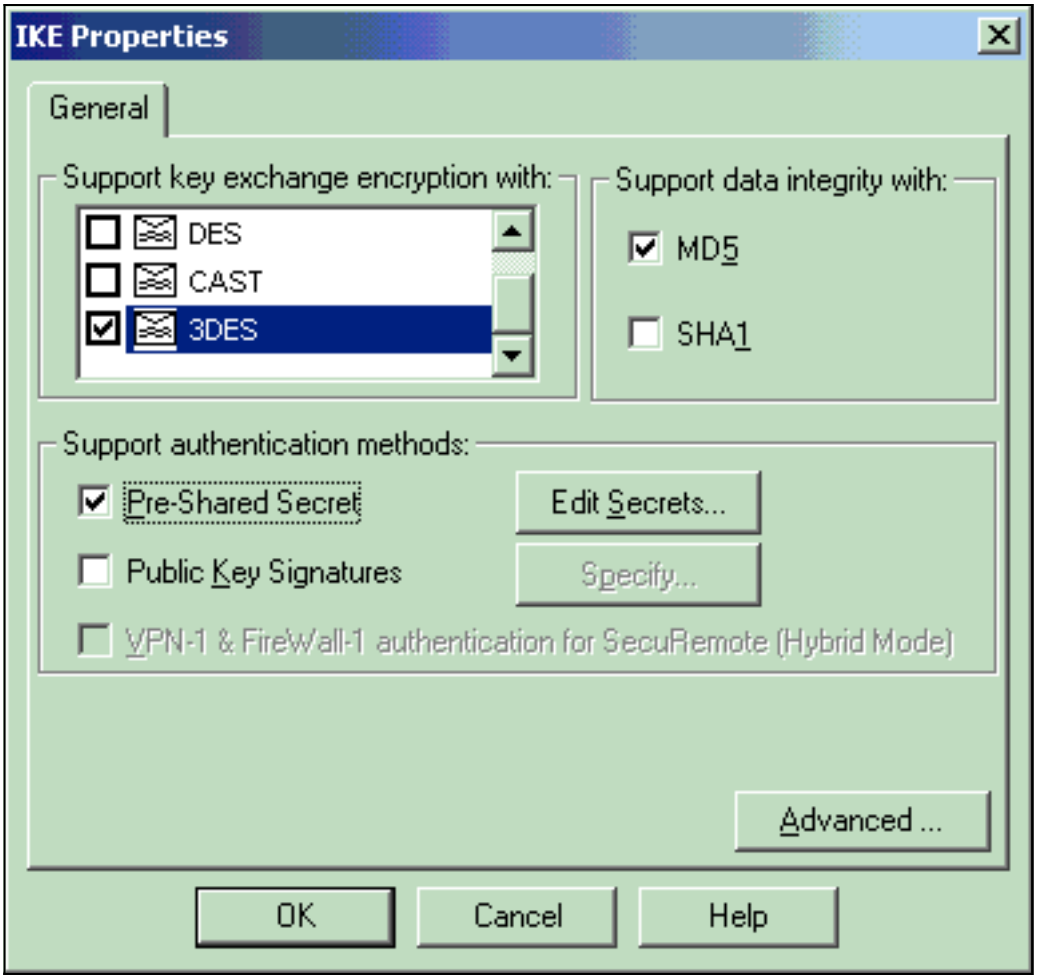
5. [Workstation Properties]ウィンドウで、インターネットに接続するCheckpoint NGの外部インターフェイスを選択し、[**Edit**]をクリックしてインターフェイスのプロパティを設定します。トポロジを外部として指定するオプションを選択し、[**OK**]をクリックします。



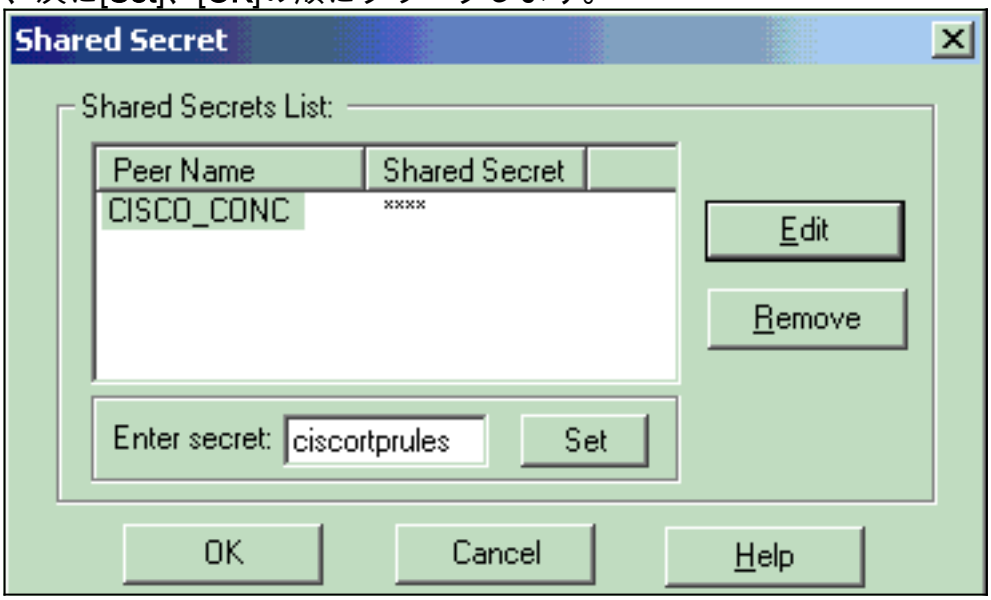
6. Checkpoint NGのWorkstation Propertiesウィンドウで、ウィンドウの左側にある選択肢から**VPNを選択**し、次に暗号化および認証アルゴリズムのIKEパラメータを選択します。[**Edit**]をクリックして、IKEプロパティを設定します。



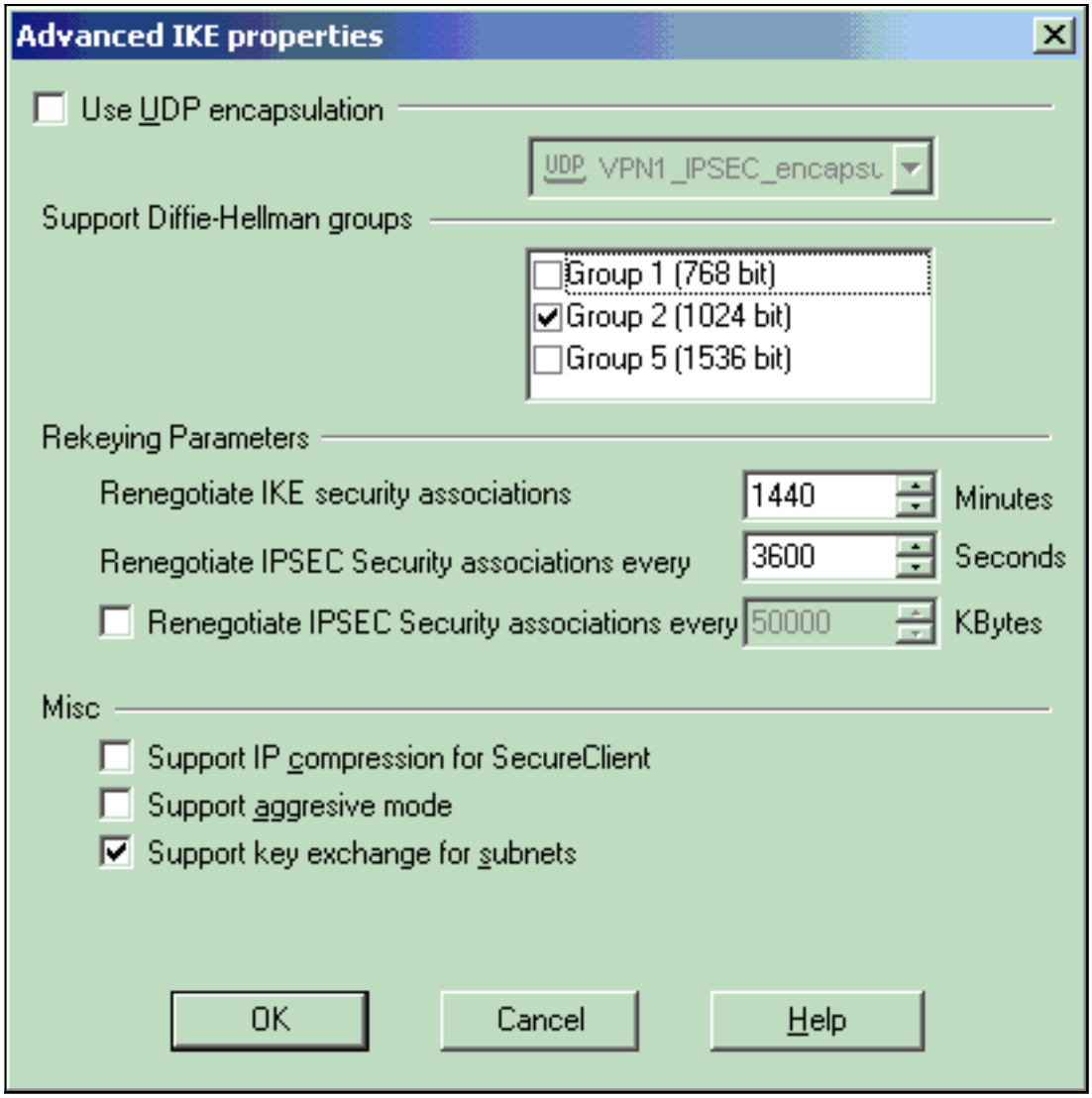
7. VPNコンセントレータのプロパティと一致するようにIKEプロパティを設定します。この例では、3DESの暗号化オプション**とMD5のハッシング**オプションを選択**します。**



8. **Pre-Shared Secrets**の認証オプションを選択し、**Edit Secrets**をクリックして、VPNコンセントレータの事前共有キーと互換性のある事前共有キーを設定します。[Edit]をクリックして、次に[Set]、[OK]の順にクリックします。

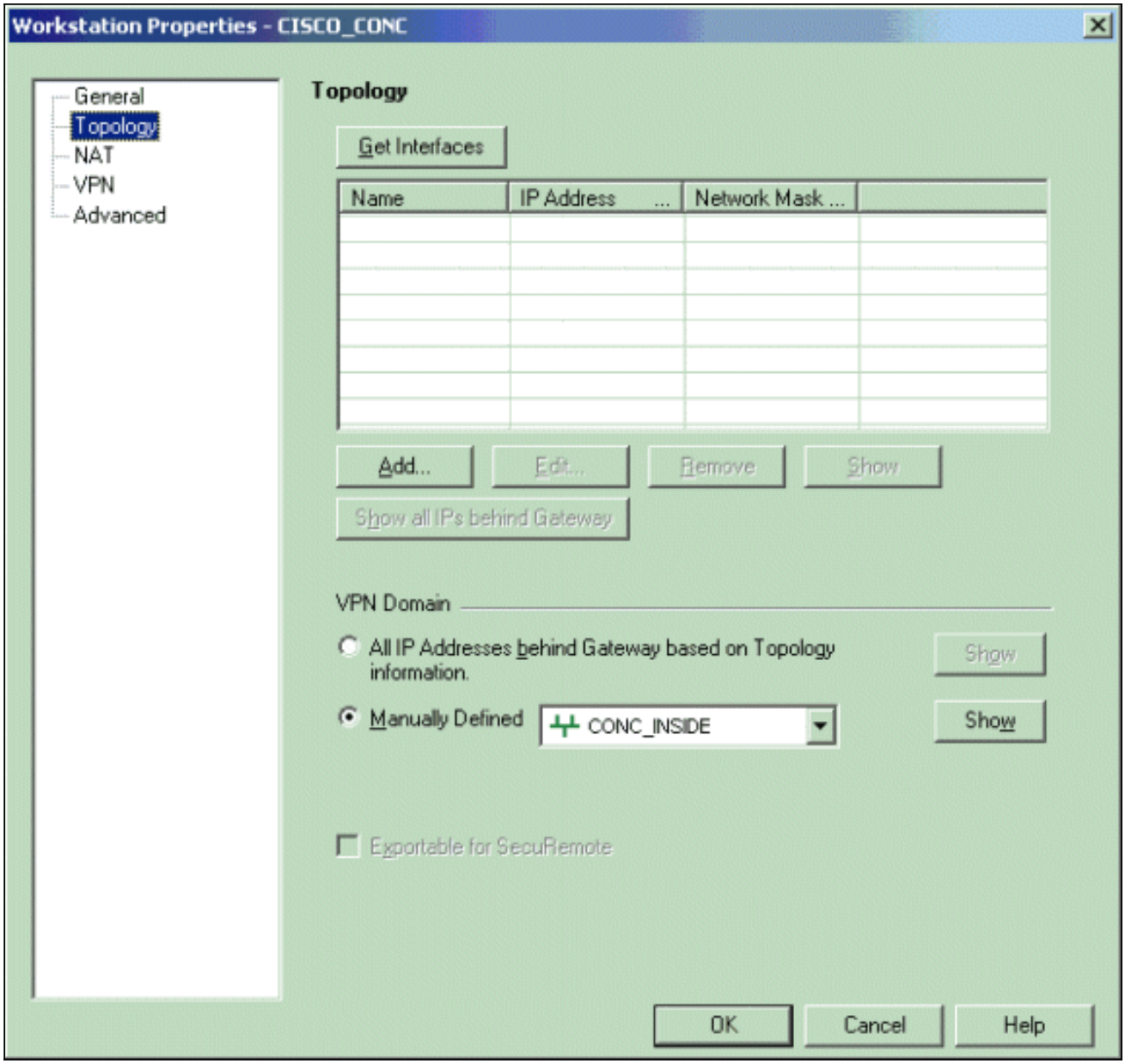


9. IKEプロパティウィンドウで、[Advanced...]をクリックし、次の設定を変更します。「アグレッシブモードをサポート」のオプションを選択解除します。[サブネットのキー交換をサポートする]オプションを選択します。終了したら、「OK」、「OK」の順にクリックします

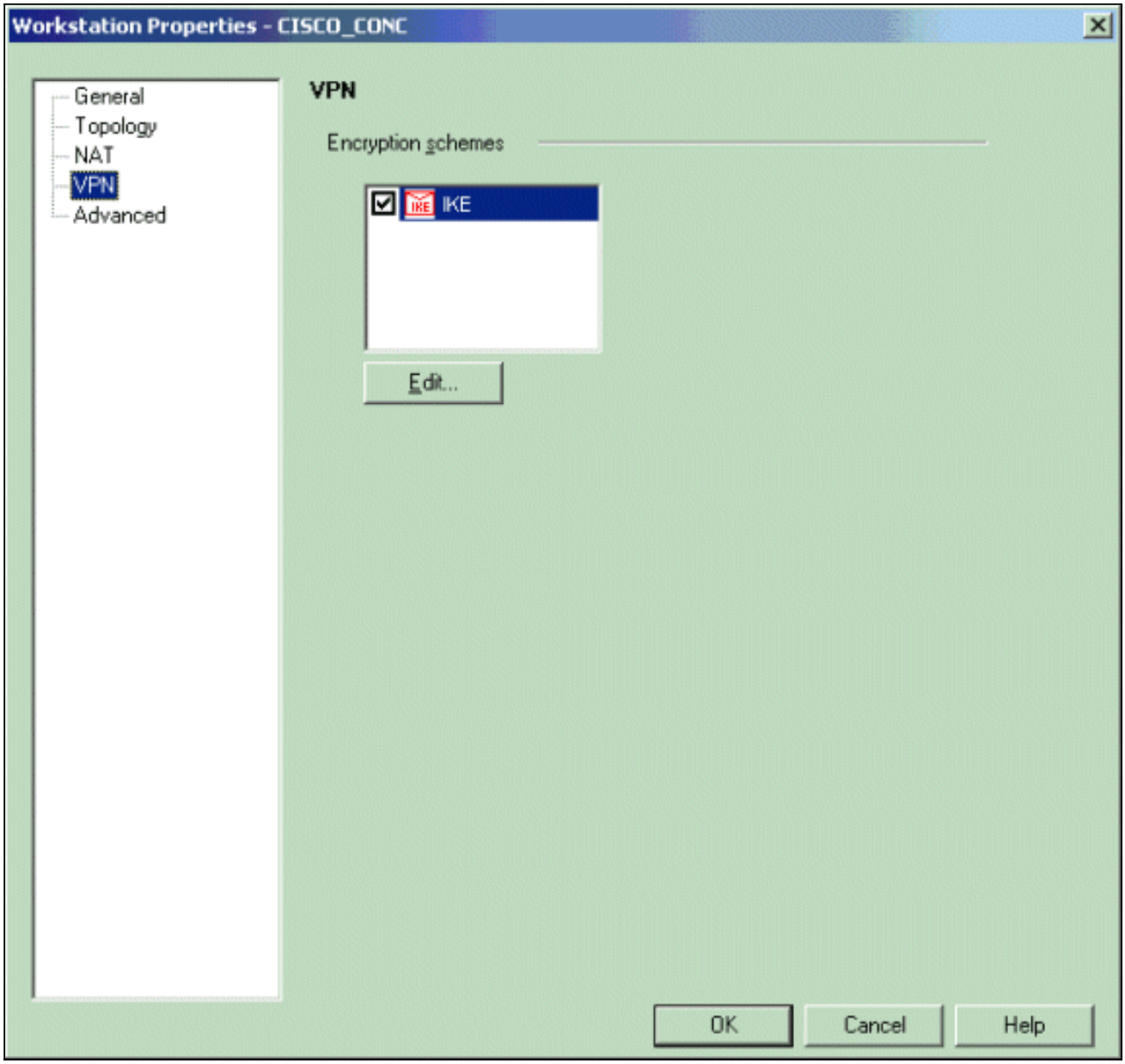


。

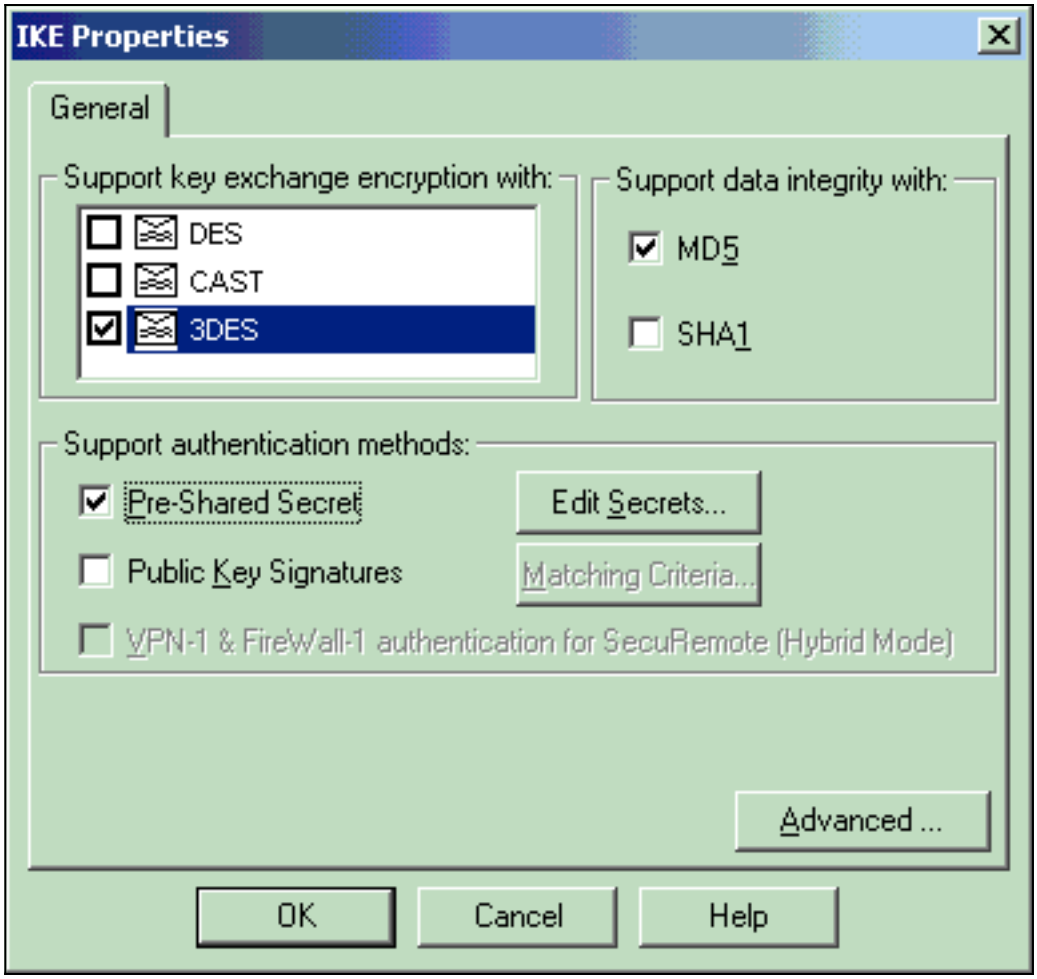
10. **[Manage] > [Network Objects] > [Edit]に移動**し、VPNコンセントレータの[Workstation Properties]ウィンドウを開きます。ウィンドウの左側の選択肢から**[Topology]**を選択し、VPNドメインを手動で定義します。この例では、CONC_INSIDE（VPNコンセントレータの内部ネットワーク）がVPNドメインとして定義されています。



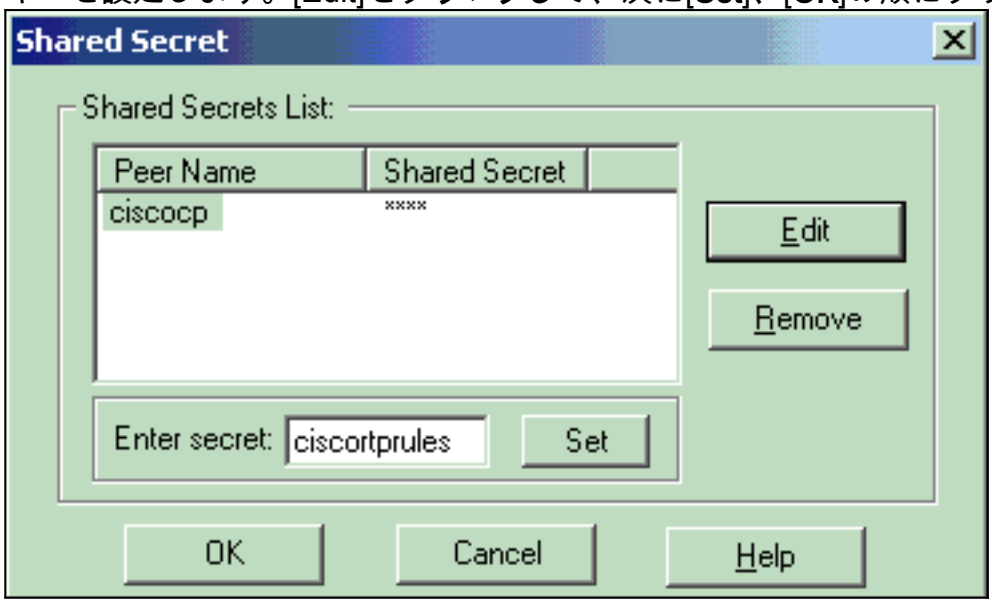
11. ウィンドウの左側の選択肢から[VPN]を選択し、暗号化方式として[**IKE**]を選択します。[**Edit**]をクリックして、IKEプロパティを設定します。



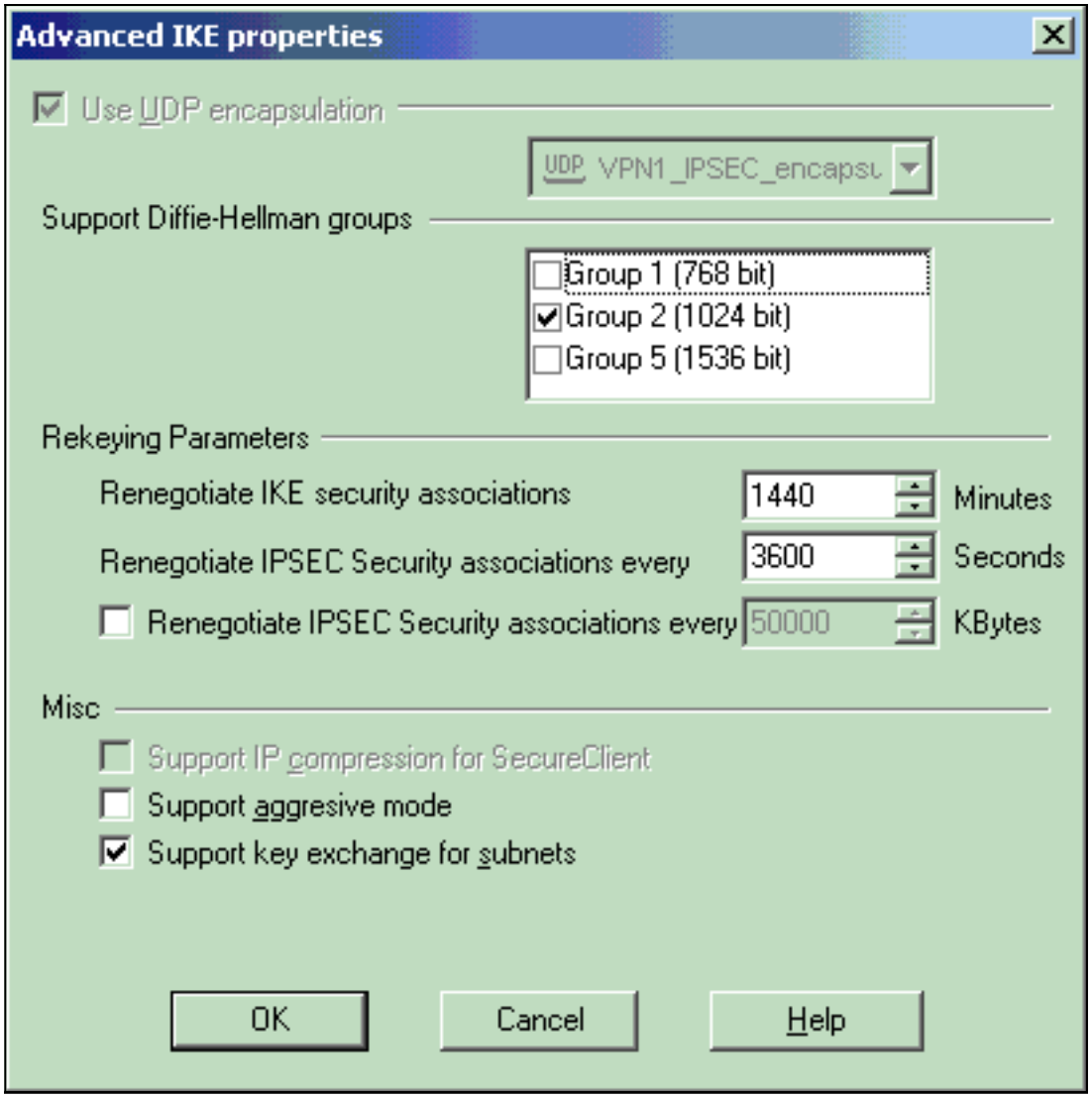
12. VPNコンセントレータの現在の設定を反映するようにIKEプロパティを設定します。この例では、3DESの暗号化オプションと**MD5のハッシング**オプションを設定します。



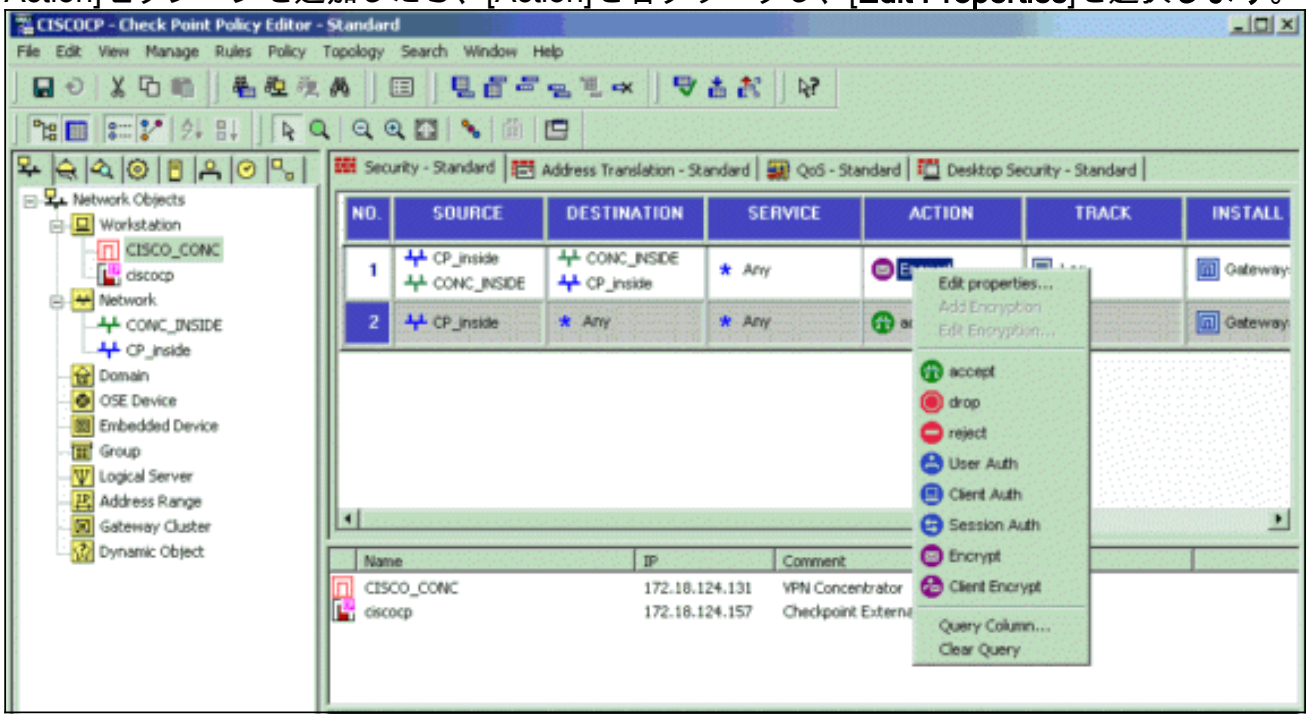
13. [Pre-Shared Secrets]の認証オプション**を選択して**、[**Edit Secrets**]をクリックして事前共有キーを設定します。[Edit]**をクリックして**、次に[**Set**]、[**OK**]の順にクリックします。



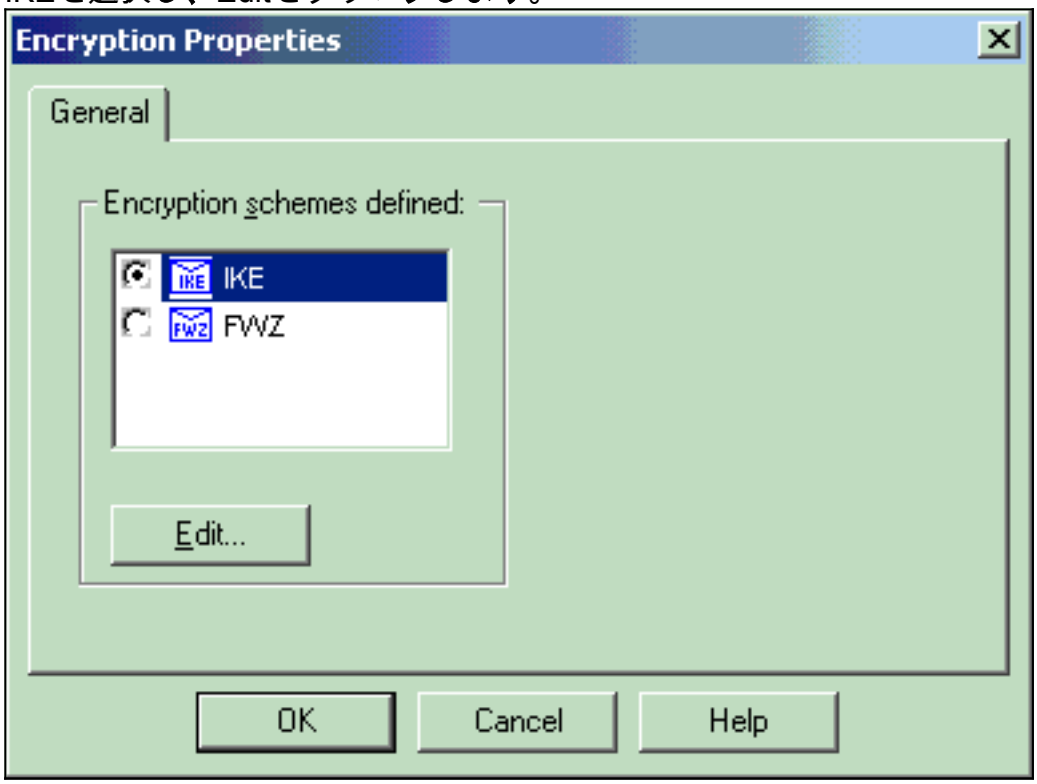
14. IKEプロパティウィンドウで、[**Advanced...]をクリック**し、次の設定を変更します。IKEプロパティに適切なDiffie-Hellmanグループを選択します。「アグレッシブモードをサポート」**のオプションを選択解除します。**[サブネットのキー交換をサポートする]**オプションを選択します。**終了したら、「OK」、「OK」**の順にク**リックします。



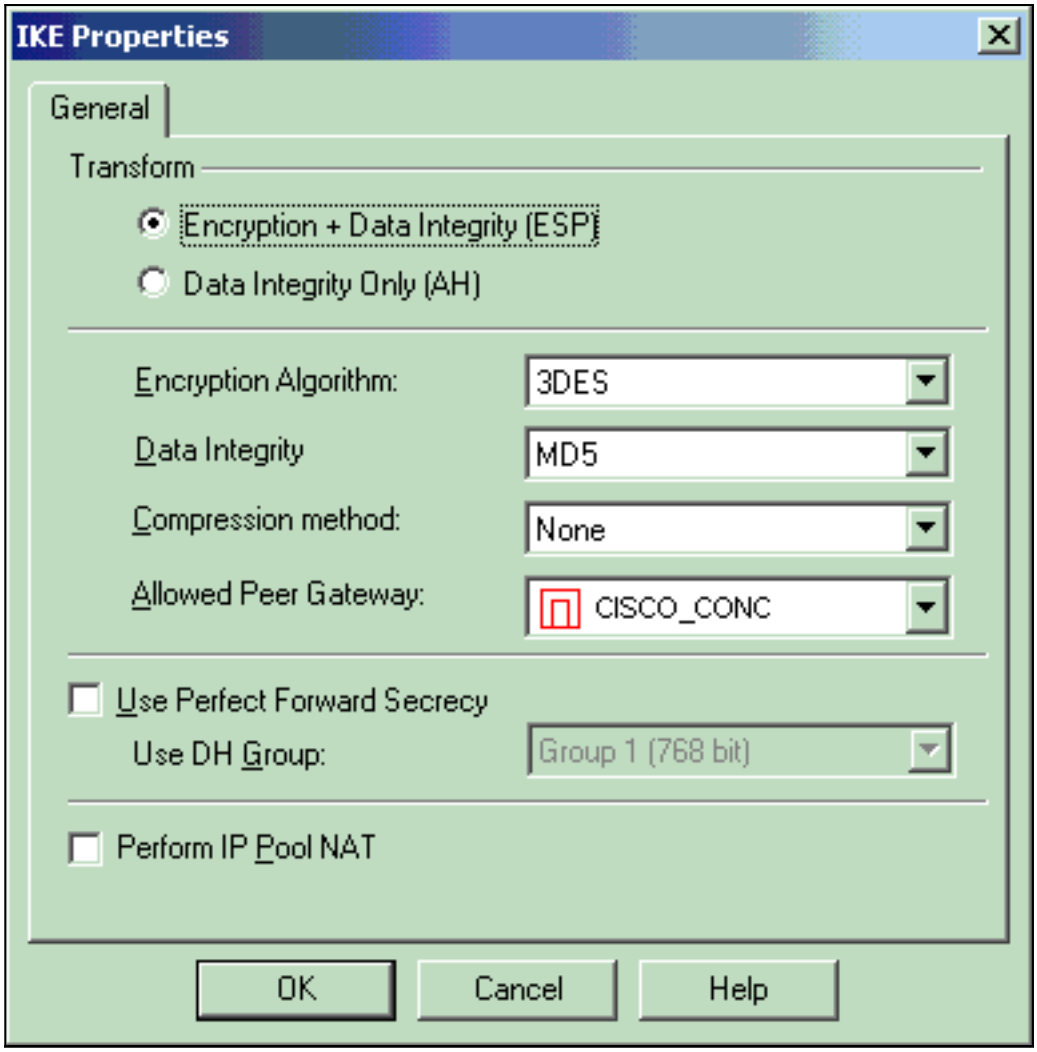
15. **[Rules] > [Add Rules] > [Top]を選択**し、ポリシーの暗号化ルールを設定します。[Policy Editor]ウィンドウで、送信元がCP_inside（Checkpoint NGの内部ネットワーク）、宛先がCONC_INSIDE（VPNコンセントレータの内部ネットワーク）のルールを挿入します。Service = **Any**、**Action = Encrypt**、**Track = Logの値を設定します**。ルールの[Encrypt Action]セクションを追加したら、[Action]を右クリックし、**[Edit Properties]を選択します**。



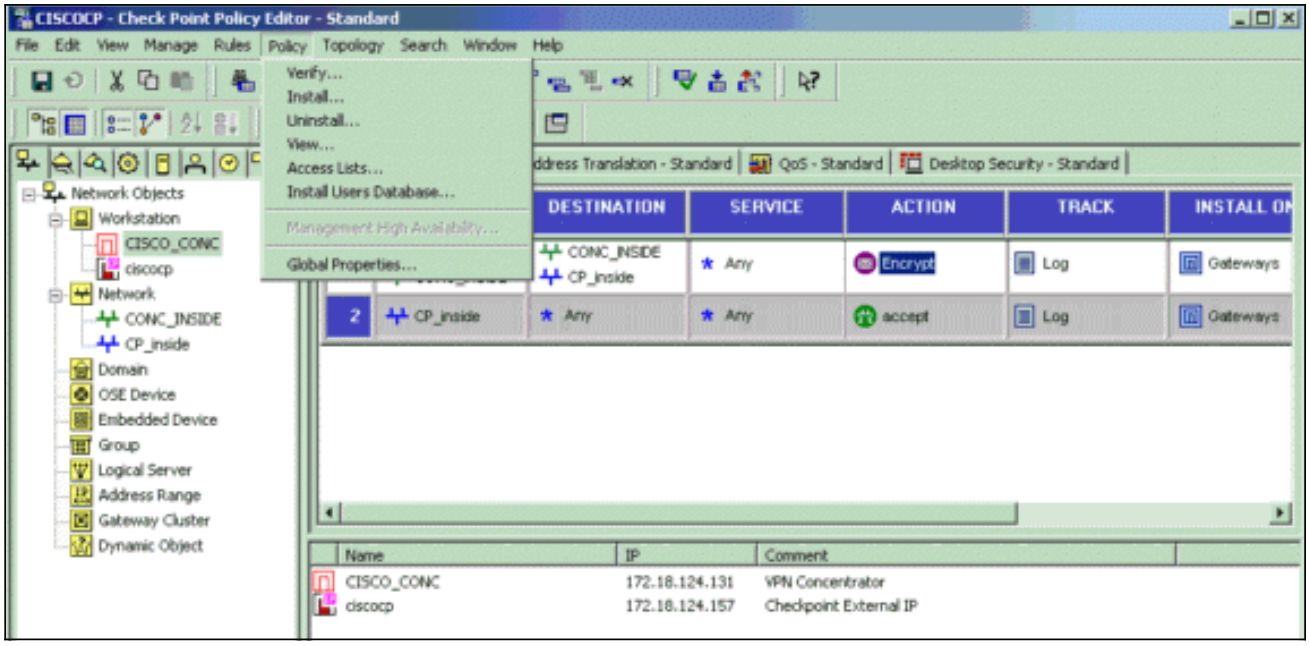
16. IKEを選択し、Editをクリックします。



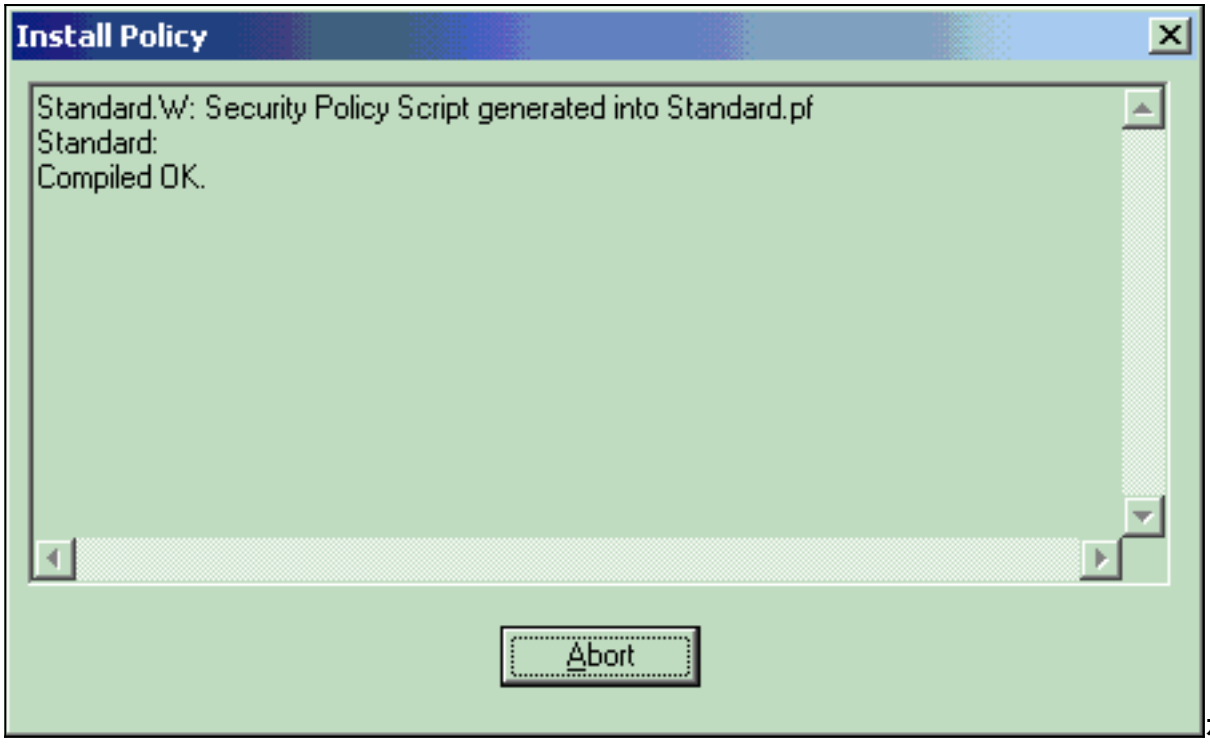
17. IKE Propertiesウィンドウで、VPN Concentratorトランスフォームと一致するようにプロパティを変更します。Transformオプションを**Encryption + Data Integrity (ESP)に設定します**。暗号化アルゴリズムを3DESに**設定します**。[Data Integrity]を[**MD5**]に設定**します**。[Allowed Peer Gateway]をVPNコンセントレータ(CISCO_CONC)と一致するように設定します。設定を終えたら OK をクリックします。



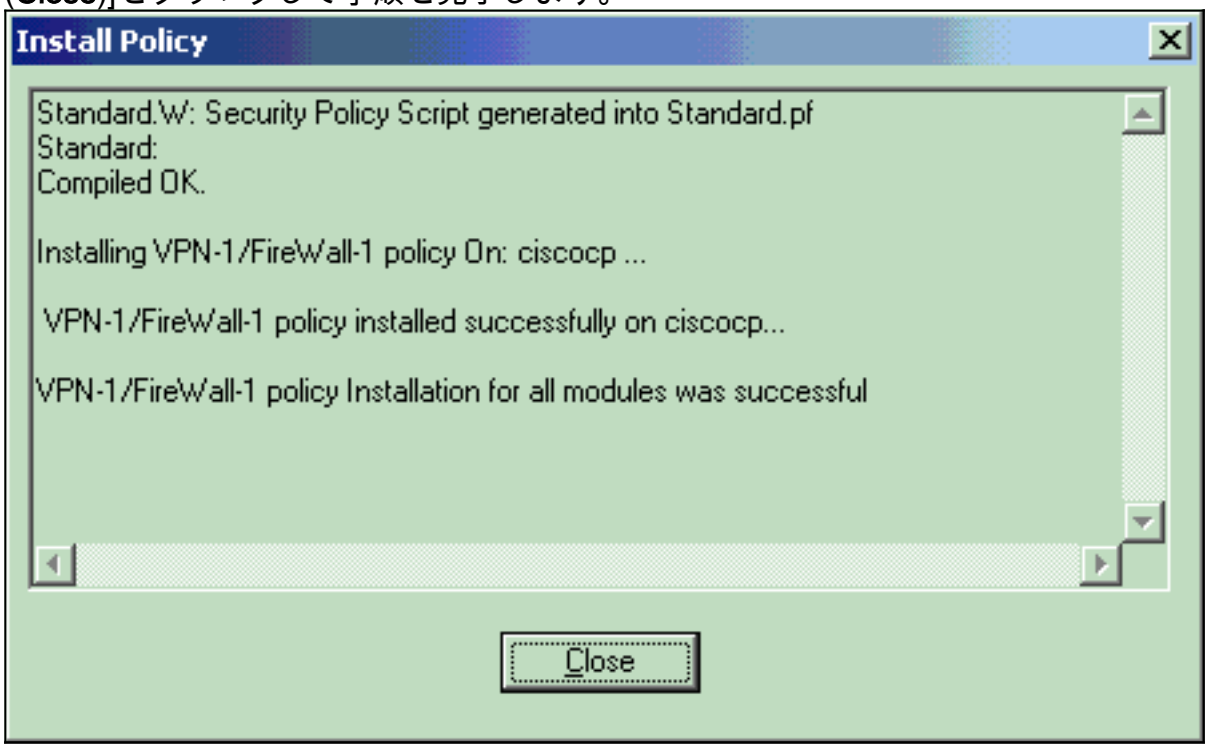
18. Checkpoint NGを設定したら、ポリシーを保存し、**[Policy] > [Install]を選択**して有効にします。



ポリシーがコンパイルされるときには、インストレーション ウィンドウに進捗状態が表示されます。



ポリシーのインストールが完了したことがインストールウィンドウに表示されたら、[閉じる(Close)]をクリックして手順を完了します。

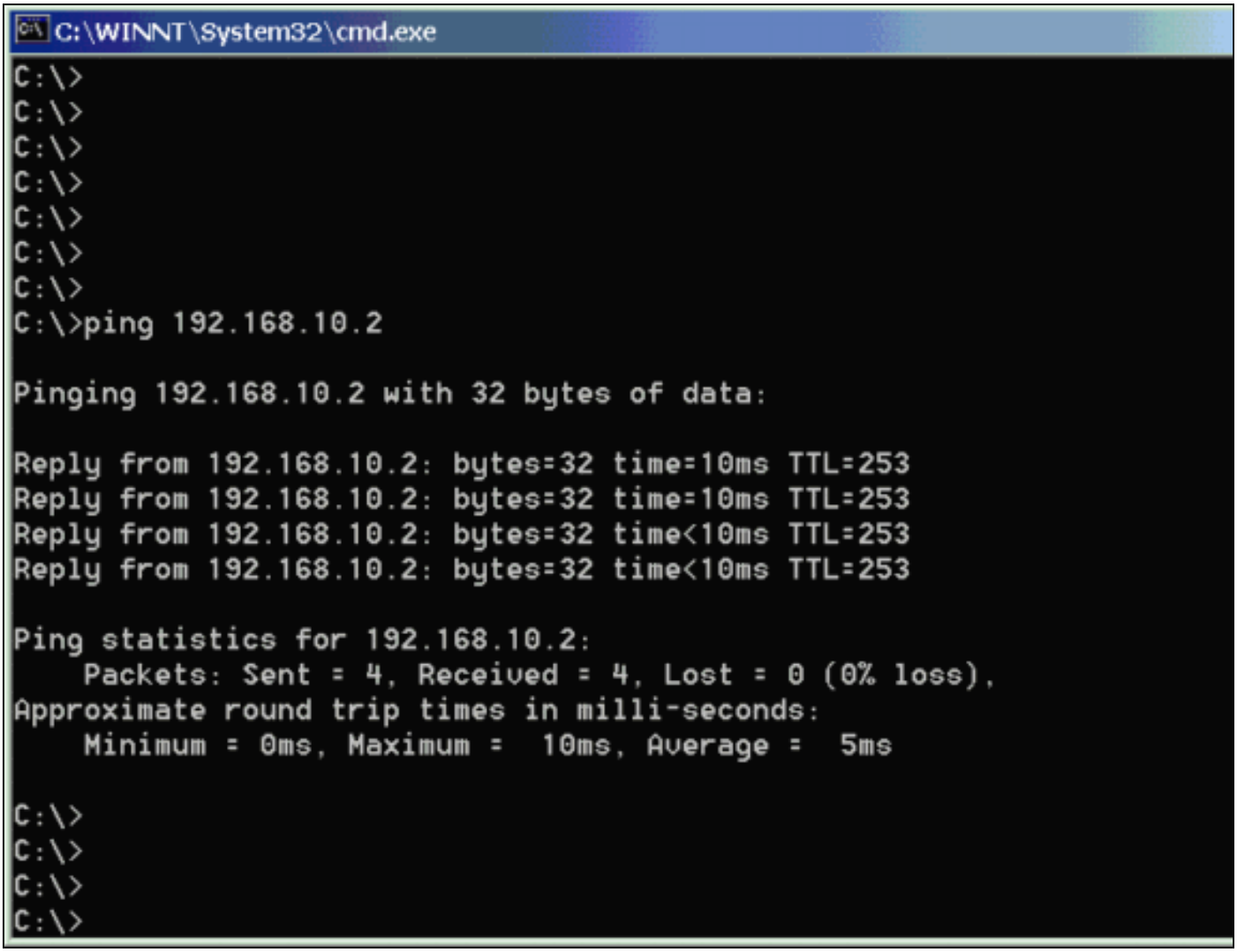


確認

ここでは、設定が正常に機能しているかどうかを確認します。

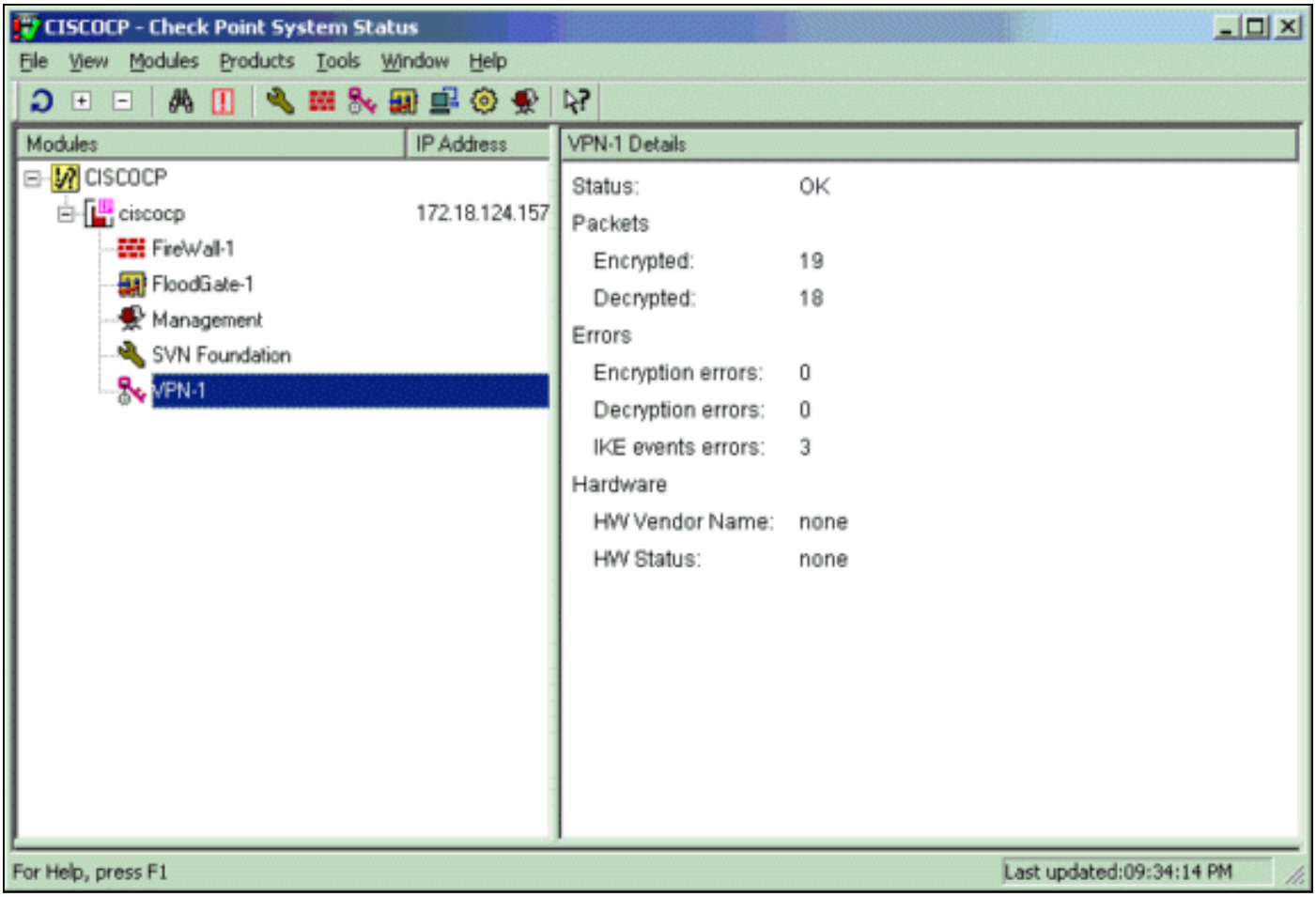
ネットワーク通信の確認

2つのプライベートネットワーク間の通信をテストするには、プライベートネットワークの1つから他のプライベートネットワークにpingを開始できます。この設定では、Checkpoint NG側(10.32.50.51)からVPNコンセントレータネットワーク(192.168.10.2)にpingが送信されました。



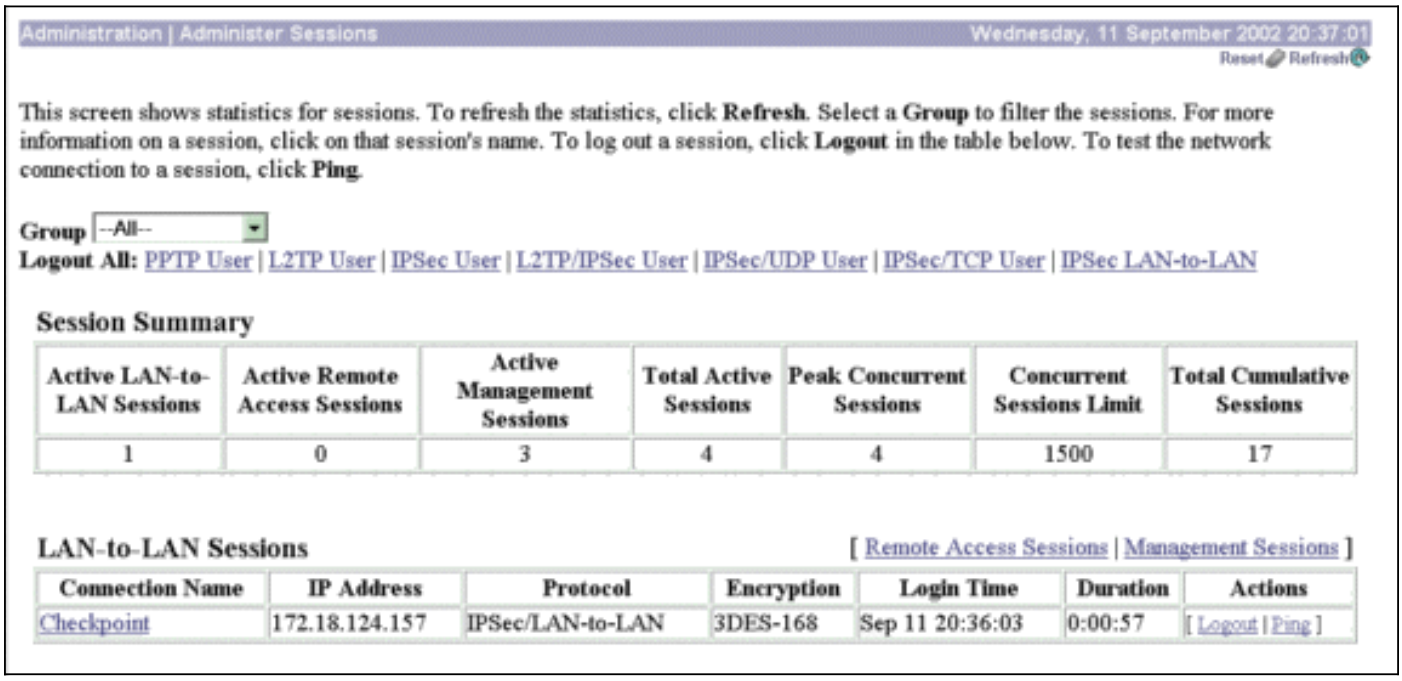
チェックポイントNGのトンネルステータスの表示

トンネルのステータスを表示するには、Policy Editorに移動し、**Window > System Status**の順に選択します。

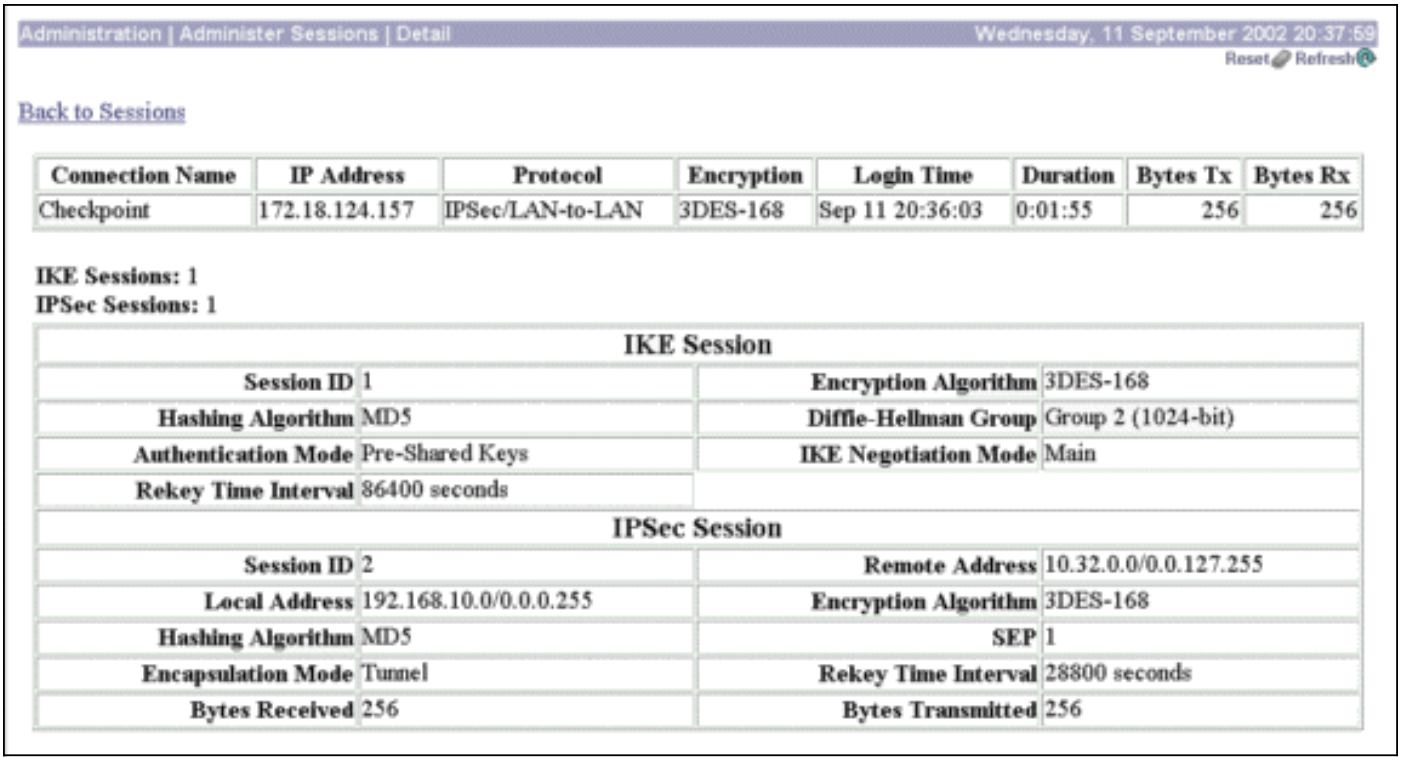


VPNコンセントレータのトンネルステータスの表示

VPNコンセントレータのトンネルステータスを確認するには、[Administration] > [Administer Sessions]の順に選択します。



[LAN-to-LAN Sessions]で、作成されたSAの詳細と送受信されたパケットの数を表示するチェックポイントの接続名を選択します。



Administration | Administer Sessions | Detail — Wednesday, 11 September 2002 20:37:59

Reset Refresh

Back to Sessions

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
Checkpoint	172.18.124.157	IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	256

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**Diffie-Hellman Group**	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys	**IKE Negotiation Mode**	Main
Rekey Time Interval	86400 seconds		
IPSec Session			
Session ID	2	**Remote Address**	10.32.0.0/0.0.127.255
Local Address	192.168.10.0/0.0.0.255	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**SEP**	1
Encapsulation Mode	Tunnel	**Rekey Time Interval**	28800 seconds
Bytes Received	256	**Bytes Transmitted**	256

トラブルシュート

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。

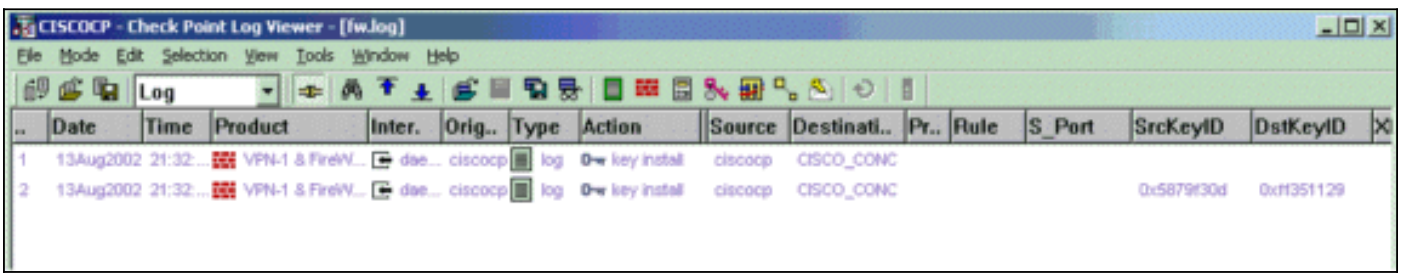
注：トラフィックは、VPNコンセントレータのパブリックIPアドレス (外部インターフェイス) を使用してIPSecトンネルを介してPATすることはできません。 そうしないと、トンネルに障害が発生します。したがって、PATに使用されるIPアドレスは、外部インターフェイスに設定されているアドレス以外のアドレスである必要があります。

ネットワーク集約

複数の隣接する内部ネットワークがチェックポイントの暗号化ドメインに設定されている場合、デバイスは対象トラフィックに関してネットワークを自動的に集約できます。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、これらのネットワークを10.0.0.0 /23に集約できます。

チェックポイントNG のデバッグ

ログを表示するには、[Window] > [Log Viewer]を選択します。



VPN コンセントレータのデバッグ

VPNコンセントレータでデバッグを有効にするには、[Configuration] > [System] > [Events] > [Classes]に移動します。重大度を1 ~ 13に設定するには、AUTH、AUTHDBG、IKE、IKEDBG、IPSEC、およびIPSECDBGを有効にします。デバッグを表示するには、[Monitoring] > [Filterable Event Log]を選択します。

```
1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128

3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157
processing SA payload

4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509
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

13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157
Oakley proposal is acceptable

14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157
processing VID payload

15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157
processing IKE SA

16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513
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

25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157
IKE SA Proposal # 1, Transform # 1 acceptable
Matches global IKE entry # 3

26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514 172.18.124.157
constructing ISA_SA for isakmp

27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157
```

```
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

31 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

33 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157
processing ke payload

34 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157
processing ISA_KE

35 09/11/2002 20:36:03.630 SEV=9 IKEDBG/1 RPT=91 172.18.124.157
processing nonce payload

36 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=520 172.18.124.157
constructing ke payload

37 09/11/2002 20:36:03.660 SEV=9 IKEDBG/1 RPT=92 172.18.124.157
constructing nonce payload

38 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=37 172.18.124.157
constructing Cisco Unity VID payload

39 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=38 172.18.124.157
constructing xauth V6 VID payload

40 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157
Send IOS VID

41 09/11/2002 20:36:03.660 SEV=9 IKEDBG/38 RPT=10 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0,
capabilities: 20000001)

43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157
constructing VID payload

44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157
Send Altiga GW VID

45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157
Generating keys for Responder...

46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) ... total length : 256

48 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60

50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157
Group [172.18.124.157]
Processing ID

51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157
Group [172.18.124.157]
processing hash

52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157
Group [172.18.124.157]
computing hash
```

```
53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157
Group [172.18.124.157]
Starting group lookup for peer 172.18.124.157

54 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/1 RPT=10
AUTH_Open() returns 9

55 09/11/2002 20:36:03.690 SEV=7 AUTH/12 RPT=10
Authentication session opened: handle = 9

56 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/3 RPT=10
AUTH_PutAttrTable(9, 748174)

57 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/6 RPT=10
AUTH_GroupAuthenticate(9, 2f1b19c, 49c648)

58 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/59 RPT=10
AUTH_BindServer(51a6b48, 0, 0)

59 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/69 RPT=10
Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1

60 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/65 RPT=10
AUTH_CreateTimer(51a6b48, 0, 0)

61 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/72 RPT=10
Reply timer created: handle = 4B0018

62 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/61 RPT=10
AUTH_BuildMsg(51a6b48, 0, 0)

63 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/64 RPT=10
AUTH_StartTimer(51a6b48, 0, 0)

64 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/73 RPT=10
Reply timer started: handle = 4B0018, timestamp = 1163319,
timeout = 30000

65 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/62 RPT=10
AUTH_SndRequest(51a6b48, 0, 0)

66 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/50 RPT=19
IntDB_Decode(3825300, 156)

67 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=19
IntDB_Xmt(51a6b48)

68 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/71 RPT=10
xmit_cnt = 1

69 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=20
IntDB_Xmt(51a6b48)

70 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/49 RPT=10
IntDB_Match(51a6b48, 3eb7ab0)

71 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/63 RPT=10
AUTH_RcvReply(51a6b48, 0, 0)

72 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/50 RPT=20
IntDB_Decode(3eb7ab0, 298)

73 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/48 RPT=10
IntDB_Rcv(51a6b48)
```

```
74 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/66 RPT=10
AUTH_DeleteTimer(51a6b48, 0, 0)

75 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/74 RPT=10
Reply timer stopped: handle = 4B0018, timestamp = 1163329

76 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/58 RPT=10
AUTH_Callback(51a6b48, 0, 0)

77 09/11/2002 20:36:03.790 SEV=6 AUTH/41 RPT=10 172.18.124.157
Authentication successful: handle = 9, server = Internal,
group = 172.18.124.157

78 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=526 172.18.124.157
Group [172.18.124.157]
Found Phase 1 Group (172.18.124.157)

79 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/4 RPT=10
AUTH_GetAttrTable(9, 748420)

80 09/11/2002 20:36:03.790 SEV=7 IKEDBG/14 RPT=10 172.18.124.157
Group [172.18.124.157]
Authentication configured for Internal

81 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=19 172.18.124.157
Group [172.18.124.157]
IKEGetUserAttributes: IP Compression = disabled

82 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=20 172.18.124.157
Group [172.18.124.157]
IKEGetUserAttributes: Split Tunneling Policy = Disabled

83 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/2 RPT=10
AUTH_Close(9)

84 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=94 172.18.124.157
Group [172.18.124.157]
constructing ID

85 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=527
Group [172.18.124.157]
construct hash payload

86 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=528 172.18.124.157
Group [172.18.124.157]
computing hash

87 09/11/2002 20:36:03.790 SEV=9 IKEDBG/46 RPT=40 172.18.124.157
Group [172.18.124.157]
constructing dpd vid payload

88 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=529 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) ... total length : 80

90 09/11/2002 20:36:03.790 SEV=4 IKE/119 RPT=10 172.18.124.157
Group [172.18.124.157]
PHASE 1 COMPLETED

91 09/11/2002 20:36:03.790 SEV=6 IKE/121 RPT=10 172.18.124.157
Keep-alive type for this connection: None

92 09/11/2002 20:36:03.790 SEV=6 IKE/122 RPT=10 172.18.124.157
```

```
Keep-alives configured on but peer does not
support keep-alives (type = None)

93 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=530 172.18.124.157
Group [172.18.124.157]
Starting phase 1 rekey timer: 64800000 (ms)

94 09/11/2002 20:36:03.790 SEV=4 AUTH/22 RPT=16
User 172.18.124.157 connected

95 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/60 RPT=10
AUTH_UnbindServer(51a6b48, 0, 0)

96 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/70 RPT=10
Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0

97 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/10 RPT=10
AUTH_Int_FreeAuthCB(51a6b48)

98 09/11/2002 20:36:03.790 SEV=7 AUTH/13 RPT=10
Authentication session closed: handle = 9

99 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=531 172.18.124.157
RECEIVED Message (msgid=54796f76) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

102 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=532 172.18.124.157
Group [172.18.124.157]
processing hash

103 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=533 172.18.124.157
Group [172.18.124.157]
processing SA payload

104 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=95 172.18.124.157
Group [172.18.124.157]
processing nonce payload

105 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=96 172.18.124.157
Group [172.18.124.157]
Processing ID

106 09/11/2002 20:36:03.790 SEV=5 IKE/35 RPT=6 172.18.124.157
Group [172.18.124.157]
Received remote IP Proxy Subnet data in ID Payload:
Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0

109 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=97 172.18.124.157
Group [172.18.124.157]
Processing ID

110 09/11/2002 20:36:03.790 SEV=5 IKE/34 RPT=6 172.18.124.157
Group [172.18.124.157]
Received local IP Proxy Subnet data in ID Payload:
Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0

113 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=534
QM IsRekeyed old sa not found by addr

114 09/11/2002 20:36:03.790 SEV=5 IKE/66 RPT=8 172.18.124.157
Group [172.18.124.157]
IKE Remote Peer configured for SA: L2L: Checkpoint
```

```
115 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=535 172.18.124.157
Group [172.18.124.157]
processing IPSEC SA

116 09/11/2002 20:36:03.790 SEV=7 IKEDBG/27 RPT=8 172.18.124.157
Group [172.18.124.157]
IPSec SA Proposal # 1, Transform # 1 acceptable

117 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=536 172.18.124.157
Group [172.18.124.157]
IKE: requesting SPI!

118 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/6 RPT=39
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000,
seq 10, 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 17248580, lifetime2 0, dsId 300

122 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/1 RPT=139
Processing KEY_GETSPI msg!

123 09/11/2002 20:36:03.790 SEV=7 IPSECDBG/13 RPT=10
Reserved SPI 305440147

124 09/11/2002 20:36:03.790 SEV=8 IKEDBG/6 RPT=10
IKE got SPI from key engine: SPI = 0x1234a593

125 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=537 172.18.124.157
Group [172.18.124.157]
oakley constucting quick mode

126 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=538 172.18.124.157
Group [172.18.124.157]
constructing blank hash

127 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=539 172.18.124.157
Group [172.18.124.157]
constructing ISA_SA for ipsec

128 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=98 172.18.124.157
Group [172.18.124.157]
constructing ipsec nonce payload

129 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=99 172.18.124.157
Group [172.18.124.157]
constructing proxy ID

130 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=540 172.18.124.157
Group [172.18.124.157]
Transmitting Proxy Id:
Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0
Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0

134 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=541 172.18.124.157
Group [172.18.124.157]
constructing qm hash

135 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=542 172.18.124.157
SENDING Message (msgid=54796f76) with payloads :
HDR + HASH (8) + SA (1) ... total length : 152

137 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=543 172.18.124.157
RECEIVED Message (msgid=54796f76) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48
```

```
139 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=544 172.18.124.157
Group [172.18.124.157]
processing hash

140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545 172.18.124.157
Group [172.18.124.157]
loading all IPSEC SAs

141 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=100 172.18.124.157
Group [172.18.124.157]
Generating Quick Mode Key!

142 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157
Group [172.18.124.157]
Generating Quick Mode Key!

143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157
Group [172.18.124.157]
Loading subnet:
Dst: 192.168.10.0 mask: 255.255.255.0
Src: 10.32.0.0 mask: 255.255.128.0

146 09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157
Group [172.18.124.157]
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959

149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40
IPSEC key message parse - msgtype 1, len 606, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0,
spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140
Processing KEY_ADD msg!

154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141
key_msghdr2secassoc(): Enter

155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142
No USER filter configured

156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143
KeyProcessAdd: Enter

157 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144
KeyProcessAdd: Adding outbound SA

158 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145
KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255,
dst 10.32.0.0 mask 0.0.127.255

159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146
KeyProcessAdd: FilterIpsecAddIkeSa success

160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41
IPSEC key message parse - msgtype 3, len 327, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0,
spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

164 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=147
Processing KEY_UPDATE msg!
```

```
165 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=148
Update inbound SA addresses

166 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=149
key_msghdr2secassoc(): Enter

167 09/11/2002 20:36:03.810 SEV=7 IPSECDBG/1 RPT=150
No USER filter configured

168 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=151
KeyProcessUpdate: Enter

169 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=152
KeyProcessUpdate: success

170 09/11/2002 20:36:03.810 SEV=8 IKEDBG/7 RPT=7
IKE got a KEY_ADD msg for SA: SPI = 0x0df37959

171 09/11/2002 20:36:03.810 SEV=8 IKEDBG/0 RPT=547
pitcher: rcv KEY_UPDATE, spi 0x1234a593

172 09/11/2002 20:36:03.810 SEV=4 IKE/120 RPT=7 172.18.124.157
Group [172.18.124.157]
PHASE 2 COMPLETED (msgid=54796f76)
```

関連情報

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN 3000 シリーズ クライアントに関するサポート ページ
- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems