Checkpoint 4.1 Firewall に対する IPSec トンネル - Cisco VPN 5000 コンセントレータの設定

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。これにより、Cisco VPN 5000 コンセントレータ（192.168.1.x）内部のプライベート ネットワークが、Checkpoint 4.1 Firewall（10.32.50.x）内部のプライベート ネットワークに参加します。 ここでは、この設定を始める前に、VPN コンセントレータ内部および Checkpoint 内部からインターネットへのトラフィック（ここでは 172.18.124.X と表現しています）が流れてい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。

- Cisco VPN 5000 コンセントレータ
- Cisco VPN 5000 コンセントレータ ソフトウェア バージョン 5.2.19.0001
- 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。

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。

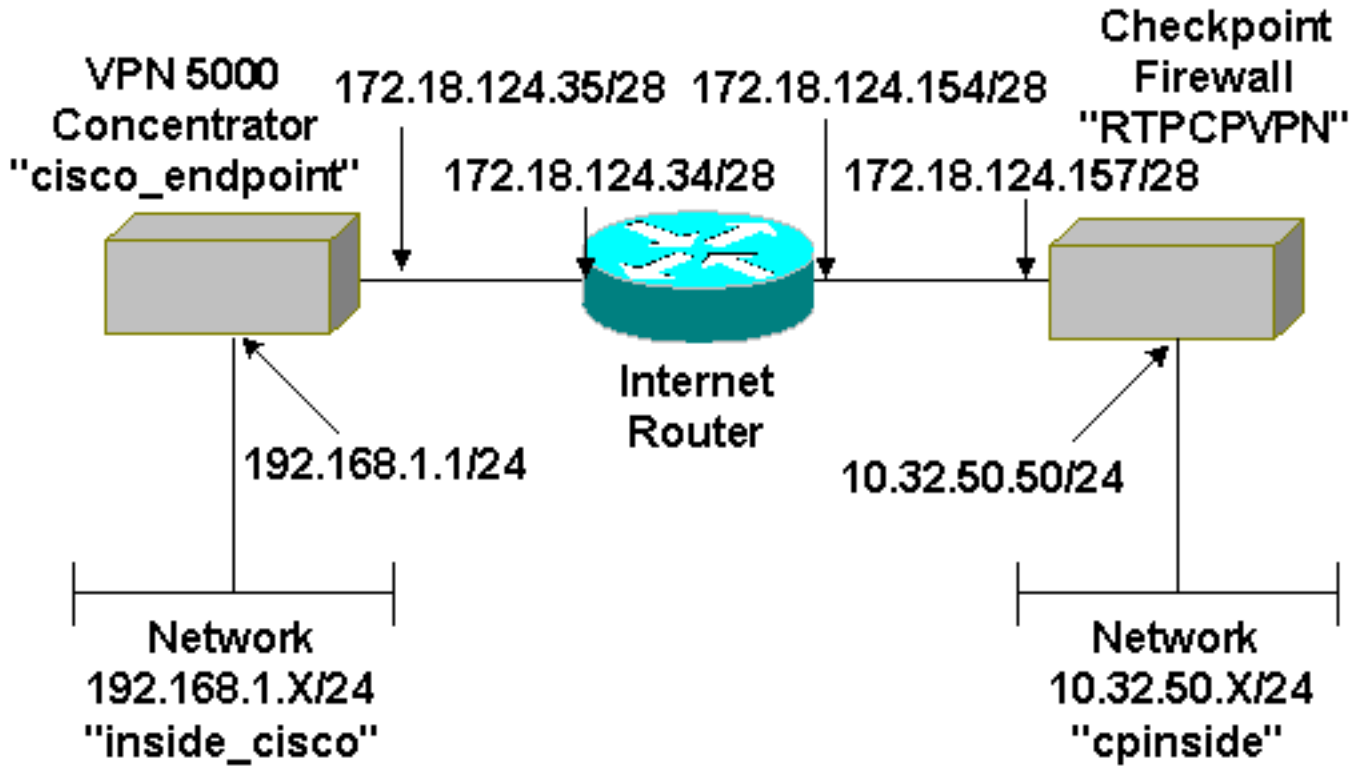
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注： このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

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。



設定

このドキュメントでは次の設定を使用します。

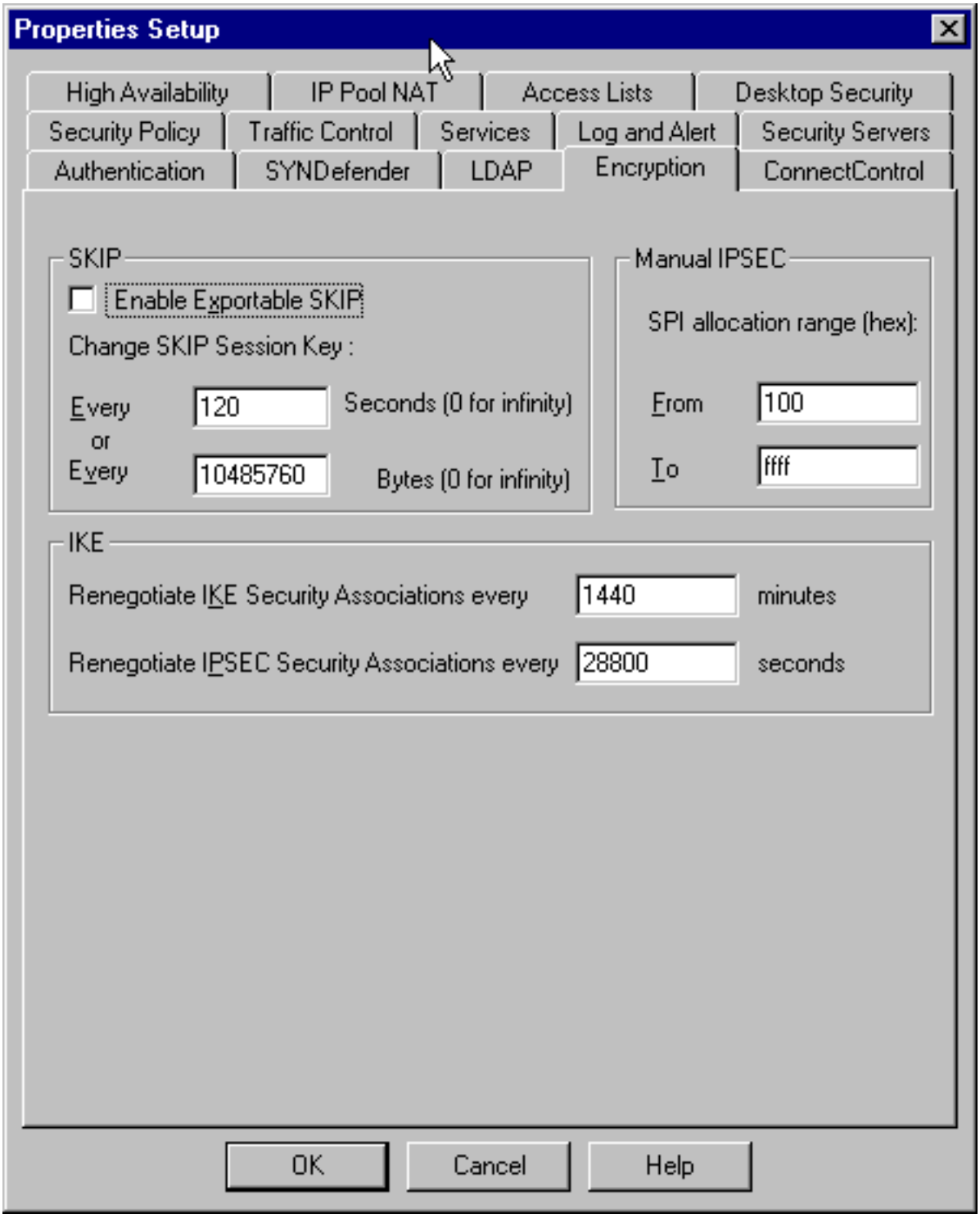
Cisco VPN 5000 コンセントレータ

```
[ IP Ethernet 0:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 192.168.1.1

[ General ]
EthernetAddress         = 00:00:a5:e9:c8:00
DeviceType              = VPN 5002/8 Concentrator
ConfiguredOn            = Timeserver not configured
ConfiguredFrom          = Command Line, from Console
DeviceName              = "cisco_endpoint"
IPSecGateway            = 172.18.124.34

[ IKE Policy ]
Protection              = SHA_DES_G2

[ Tunnel Partner VPN 1 ]
KeyLifeSecs             = 28800
LocalAccess             = "192.168.1.0/24"
Peer                    = "10.32.50.0/24"
BindTo                  = "ethernet 1:0"
SharedKey               = "ciscorules"
KeyManage               = Auto
Transform               = esp(sha,des)
Partner                 = 172.18.124.157
Mode                    = Main

[ IP VPN 1 ]
Numbered                = Off
Mode                    = Routed

[ IP Ethernet 1:0 ]
IPAddress               = 172.18.124.35
SubnetMask              = 255.255.255.240
Mode                    = Routed

[ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1

Configuration size is 1131 out of 65500 bytes.
```

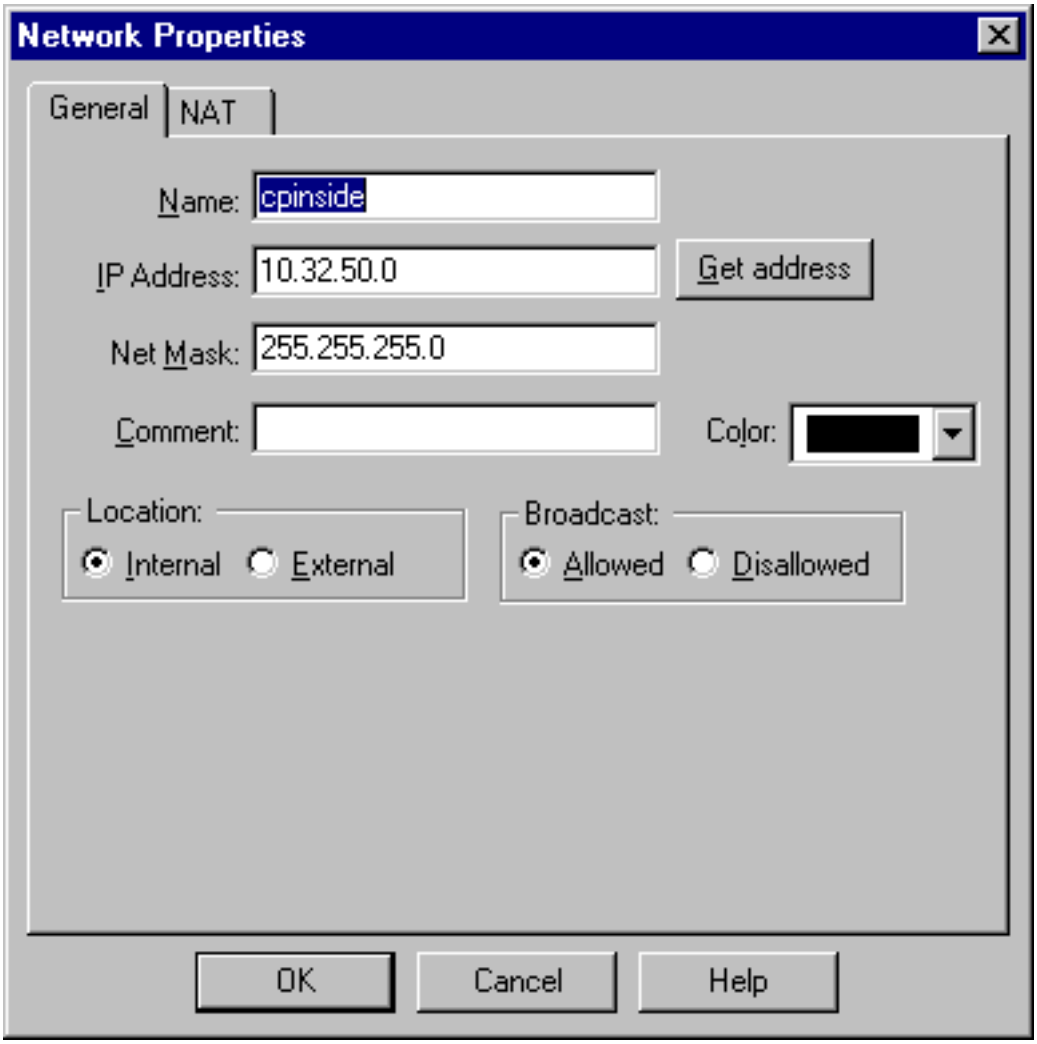
Checkpoint 4.1 Firewall

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

1. [Properties] > [Encryption] を選択し、Checkpoint IPsec ライフタイムを VPN コンセントレータ コマンドの KeyLifeSecs = 28800 と一致するように設定します。**注：チェックポイントインターネットキーエクスチェンジ(IKE)ライフタイムはデフォルトのままにします。**

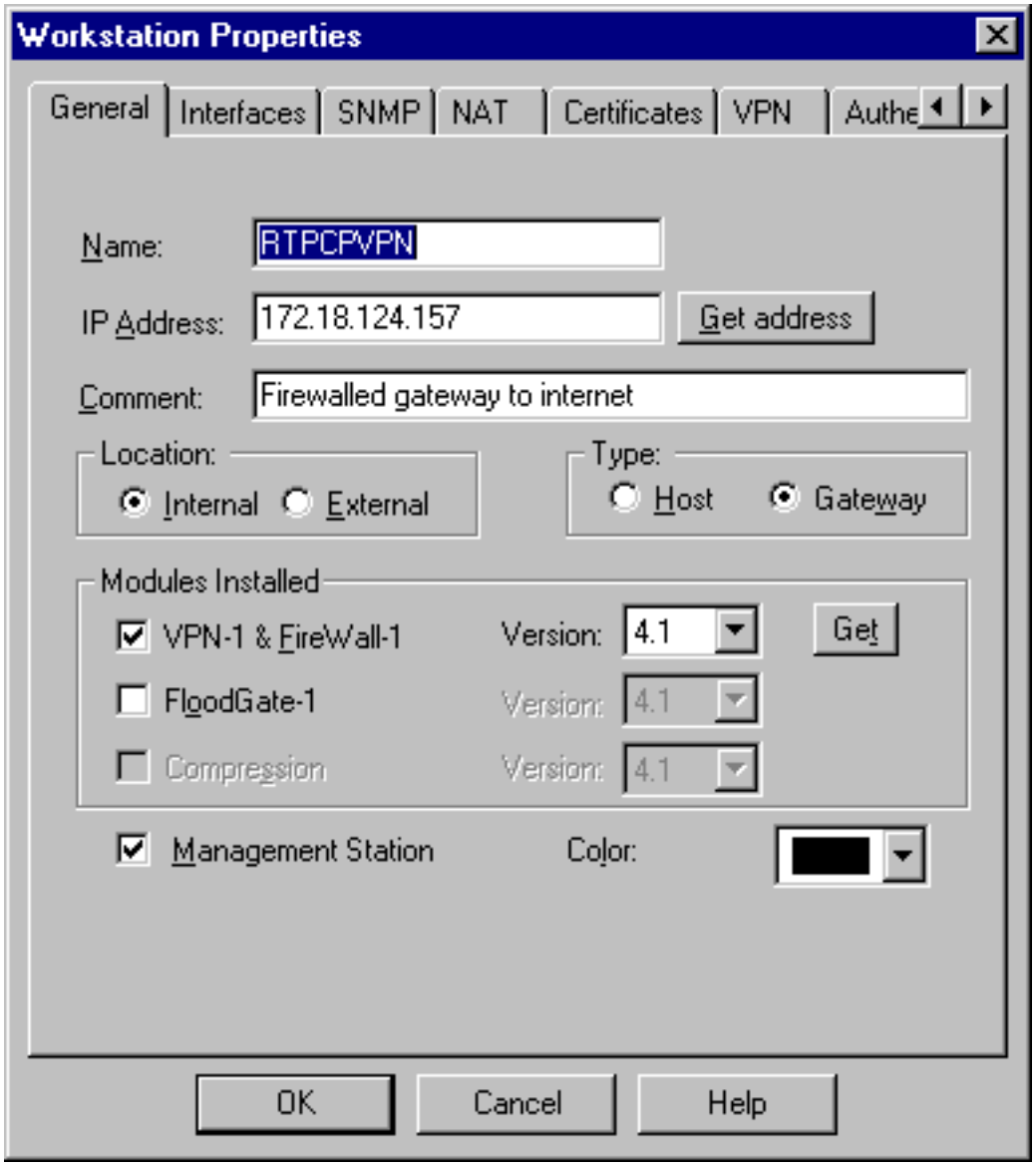


2. [Manage] > [Network objects] > [New]（または [Edit]）> [Network] の順に選択し、Checkpoint の背後にある内部（「cpinside」）ネットワークのオブジェクトを設定します。これは、VPN コンセントレータ コマンドの **Peer = "10.32.50.0/24" と一致している必要が**



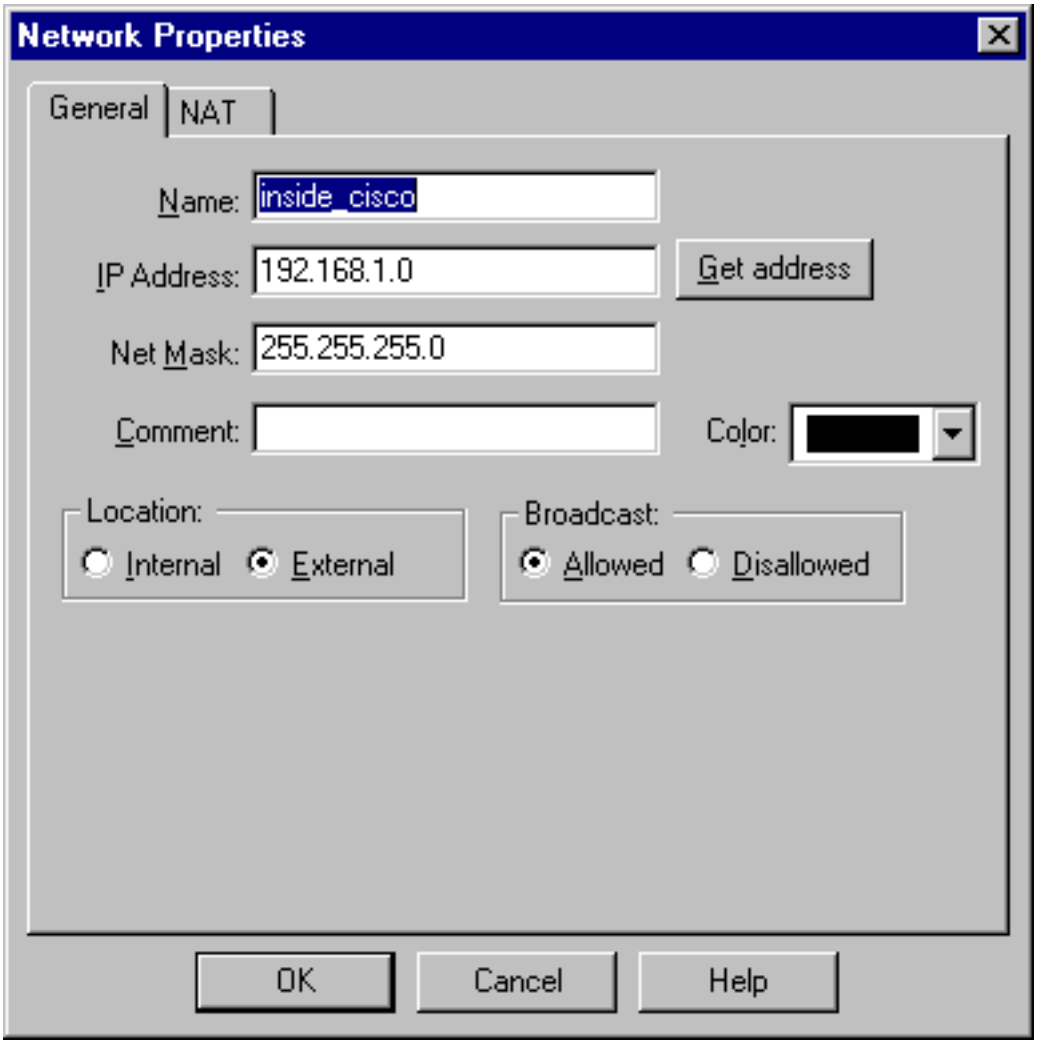
あります。

3. [Manage] > [Network objects] > [Edit] の順に選択し、VPN コンセントレータが Partner = <ip> コマンドで指し示しているゲートウェイ（「RTPCPVPN」Checkpoint）エンドポイントのオブジェクトを編集します。[Location] の [Internal] を選択します。[Type] の [Gateway] を選択します。[Modules Installed] の下で、[VPN-1 & FireWall-1] と [Management Station]

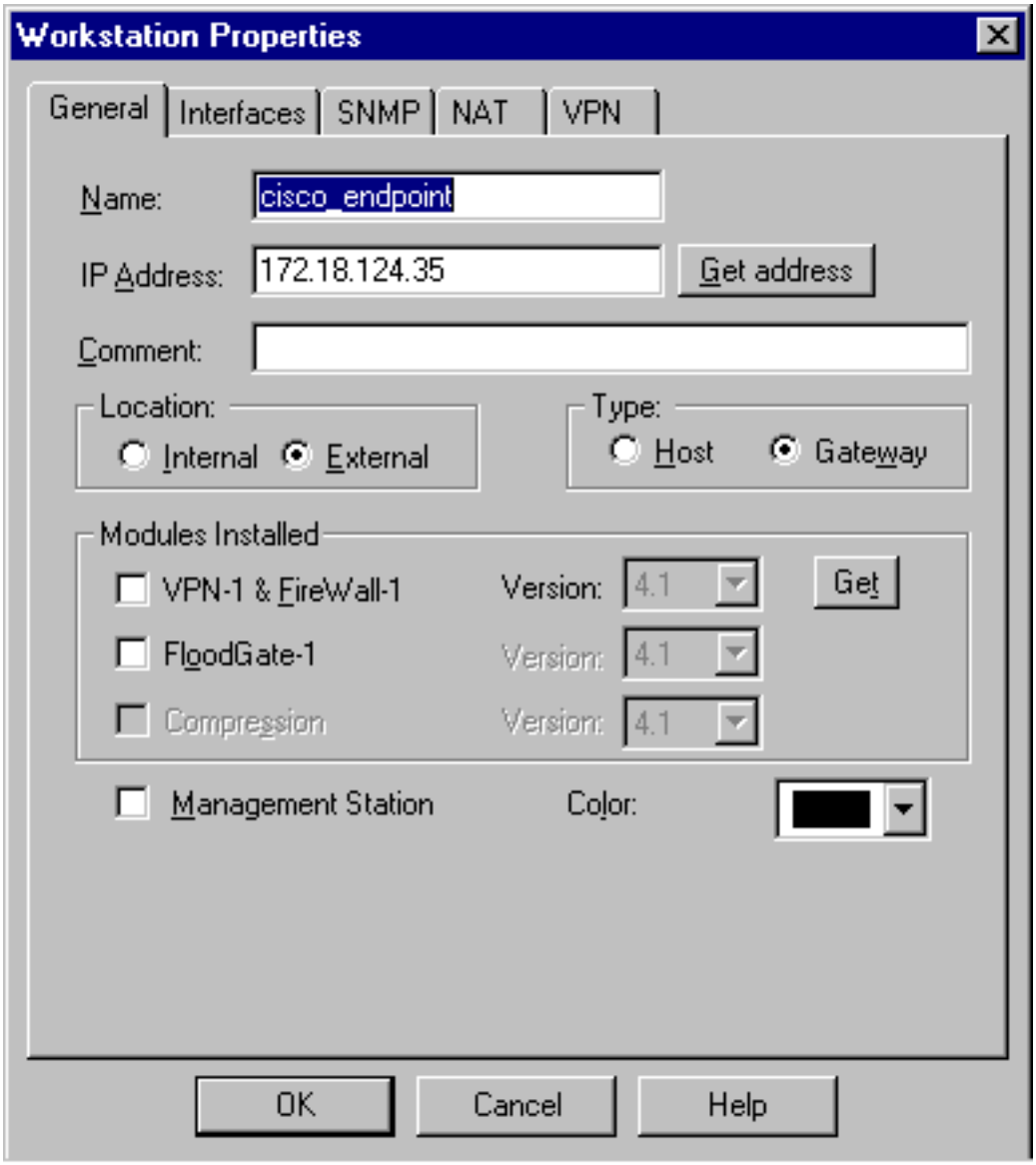


をオンにします。

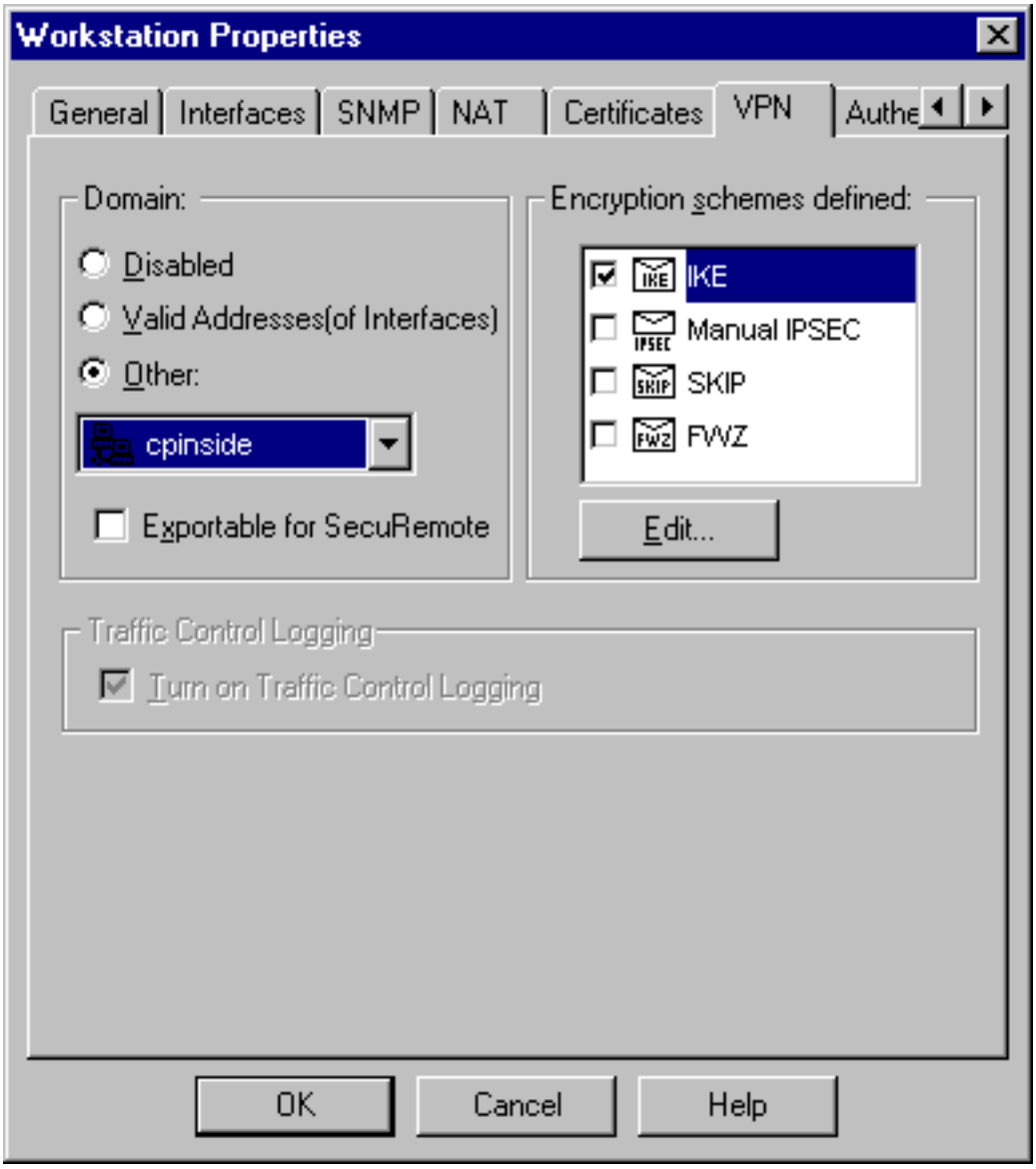
4. [Manage] > [Network objects] > [New]（または [Edit]）> [Network] の順に選択し、VPN コンセントレータの背後にある外部（「inside_cisco」）ネットワークのオブジェクトを設定します。これは、VPN コンセントレータ コマンドの **LocalAccess = <192.168.1.0/24> と一致している必要があります。**



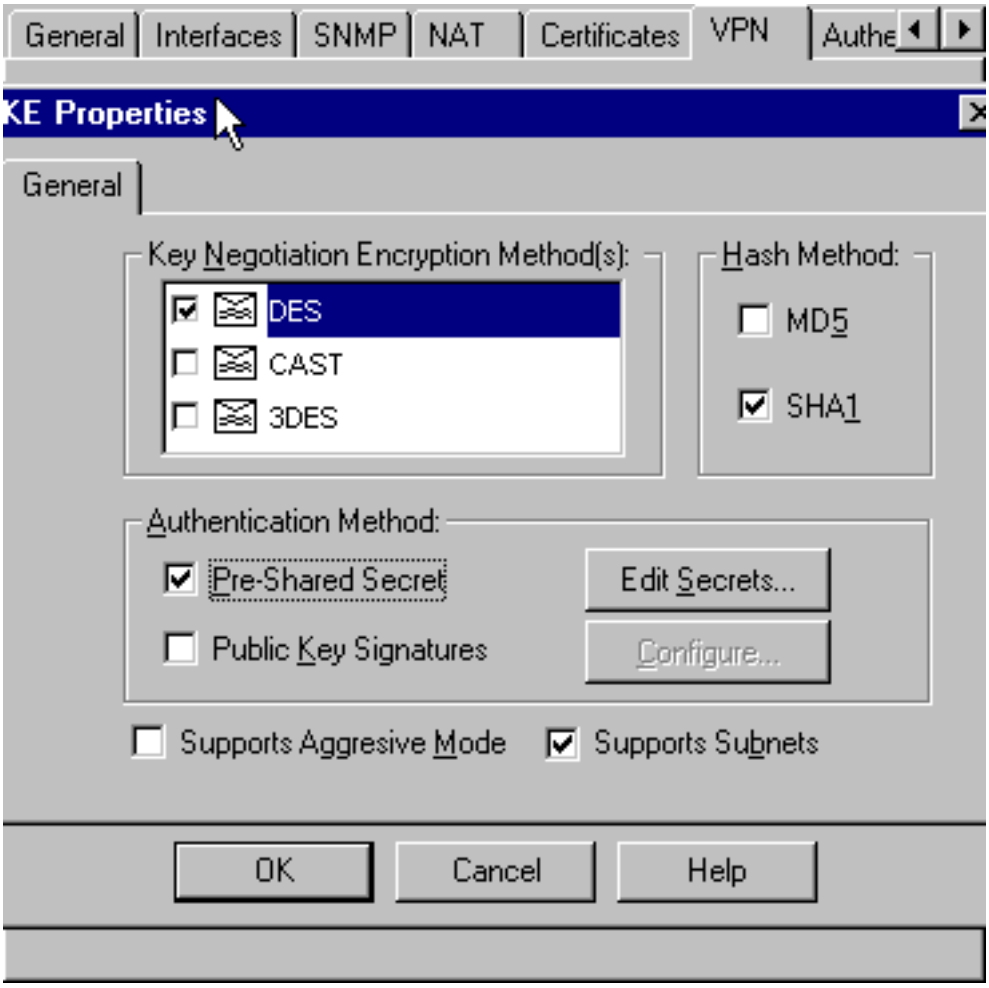
5. [Manage] > [Network objects] > [New] > [Workstation] の順に選択し、外部（「cisco_endpoint」）VPN コンセントレータ ゲートウェイのオブジェクトを追加します。これは、Checkpoint への接続を持つ VPN コンセントレータの「外部」インターフェイスです（このドキュメントでは、172.18.124.35 は **IPAddress = <ip> コマンドの IP アドレス**）。[Location] の [External] を選択します。[Type] の [Gateway] を選択します。**注**：VPN-1/FireWall-1はチェックしないでください。



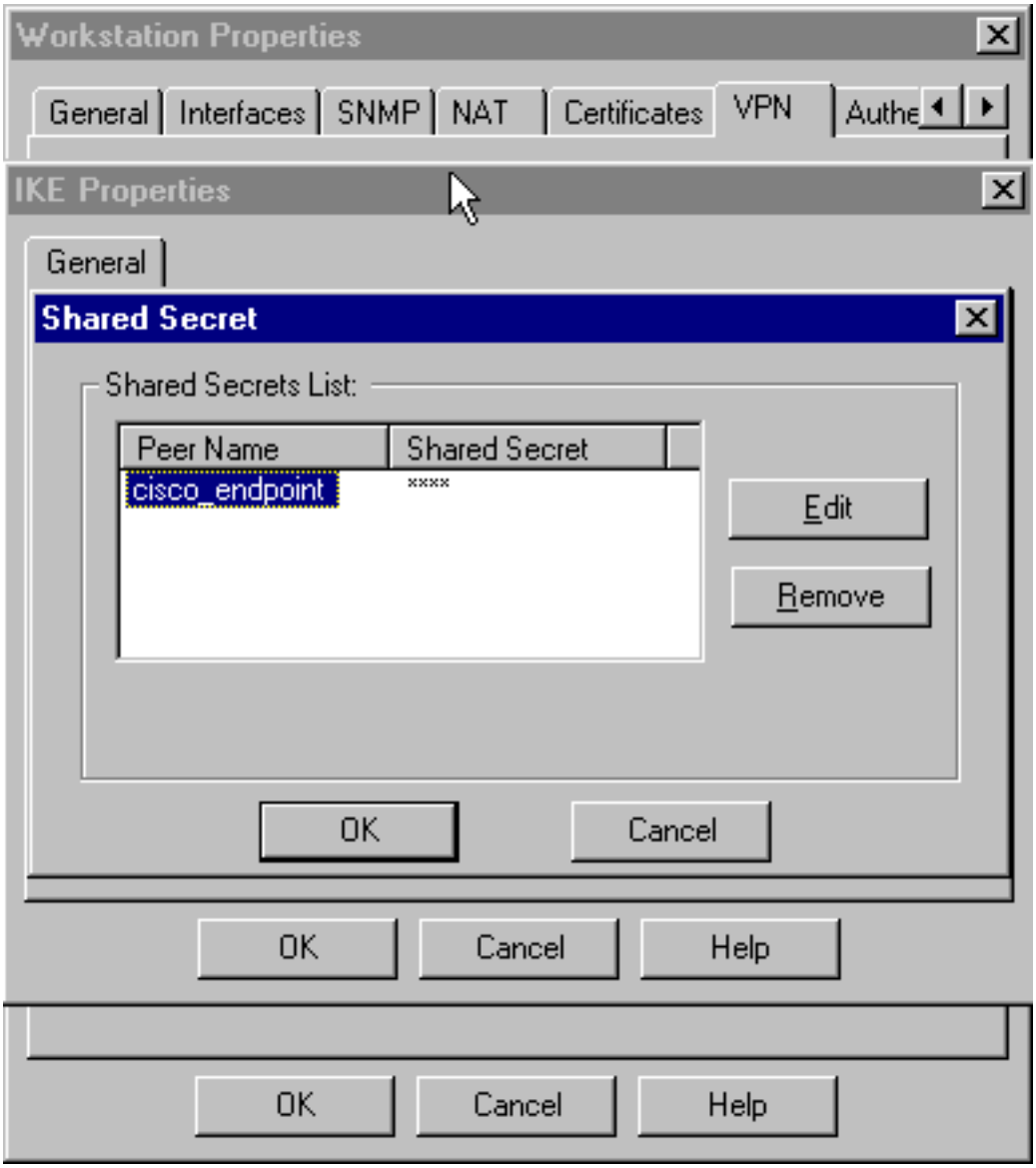
6. [Manage] > [Network objects] > [Edit] の順に選択し、Checkpoint ゲートウェイ エンドポイント（「RTPCPVPN」という名前）の [VPN] タブを編集します。[Domain] の下で、[Other] を選択してから、Checkpoint ネットワークの内側（「cpinside」という名前）をドロップダウン リストから選択します。[Encryption schemes defined] の下で、[IKE] を選択してから [Edit] をクリックします。



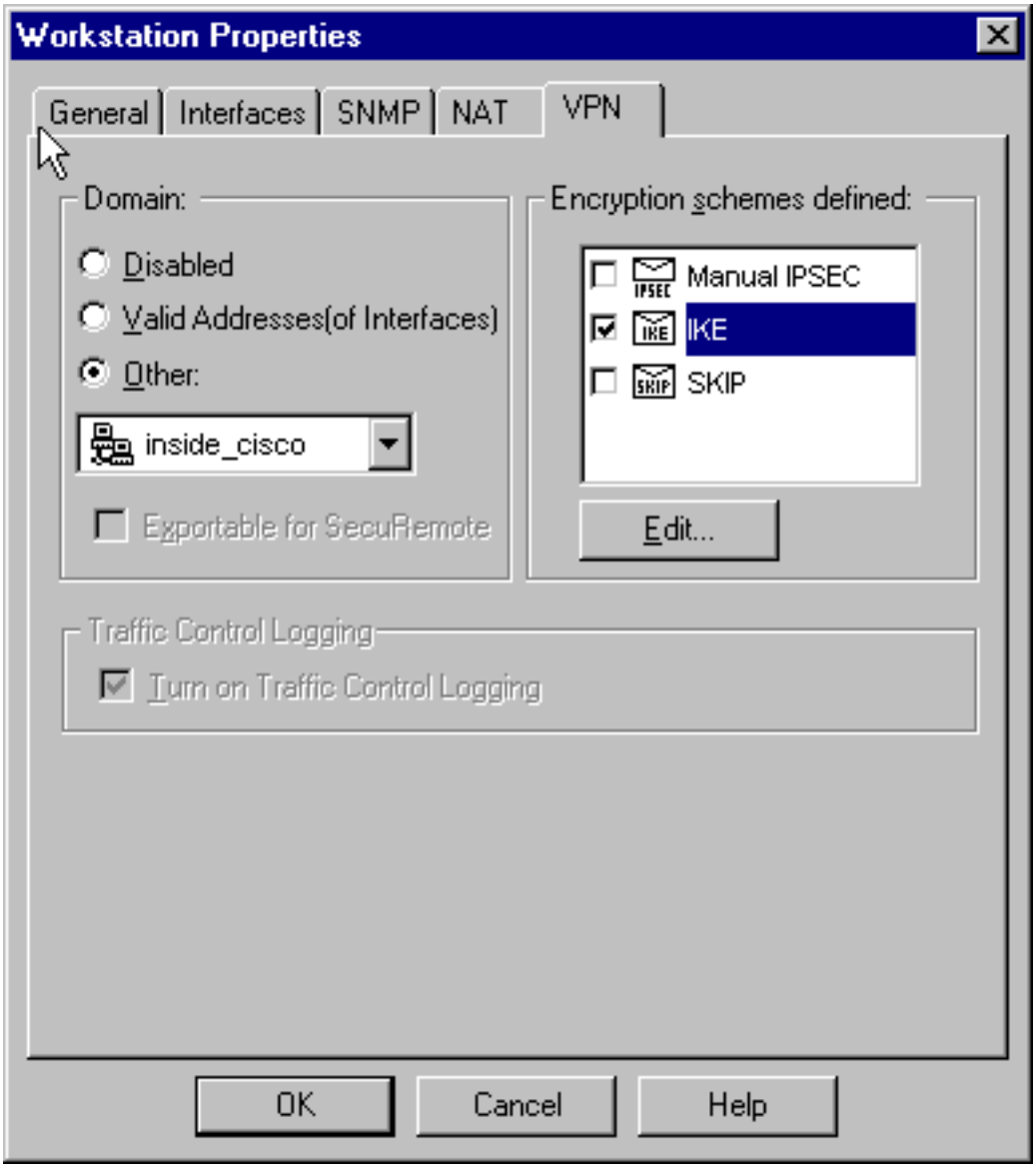
7. VPN コンセントレータ コマンドの **SHA_DES_G2 と一致するように IKE プロパティを [DES] 暗号化と [SHA1] ハッシュに変更します。注：**「G2」はDiffie-Hellmanグループ1または2を指します。テストでは、Checkpointが「G2」または「G1」を受け入れることが検出されました。次の設定を変更します。[Aggressive Mode] をオフにします。[Supports Subnets] をオンにします。[Authentication Method] の [Pre-Shared Secret] をオンにします。



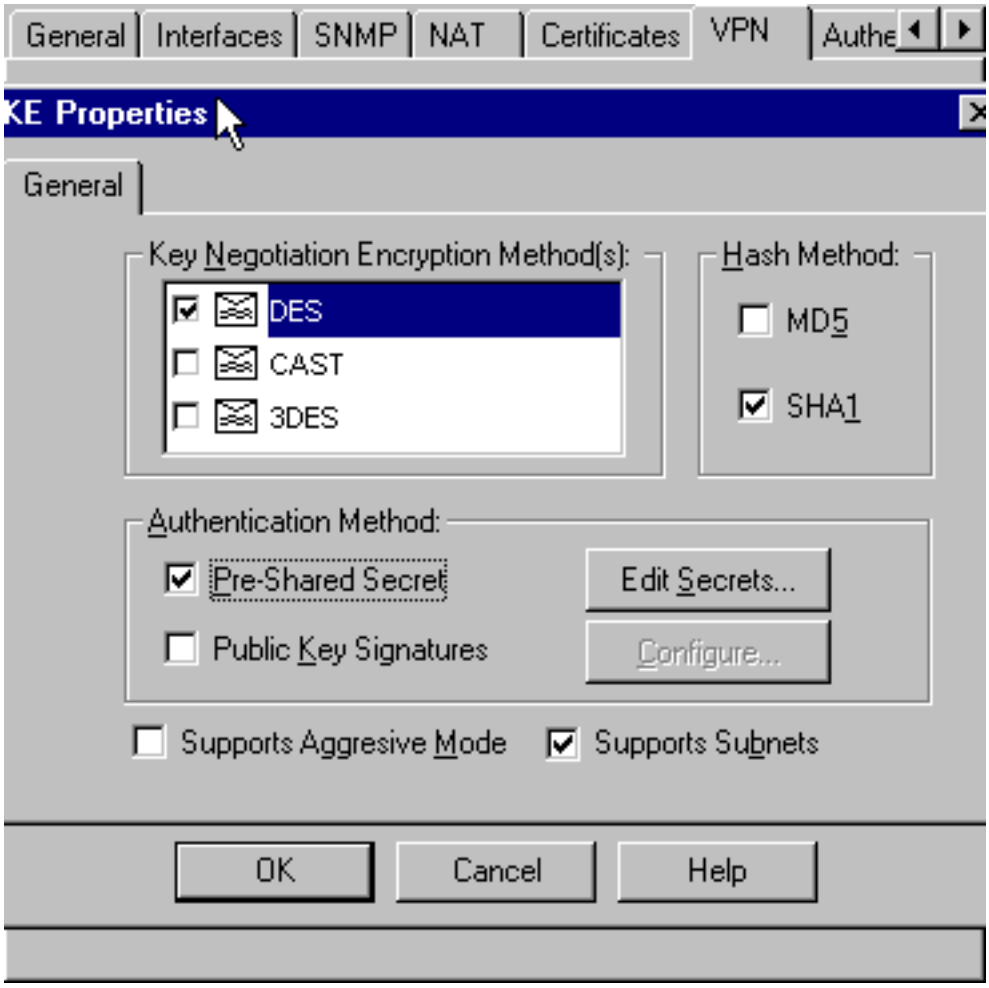
8. [Edit Secrets] をクリックし、事前共有キーを VPN コンセントレータ コマンドの SharedKey = <key> と一致するように設定します。



9. [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、VPN コンセントレータ 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。

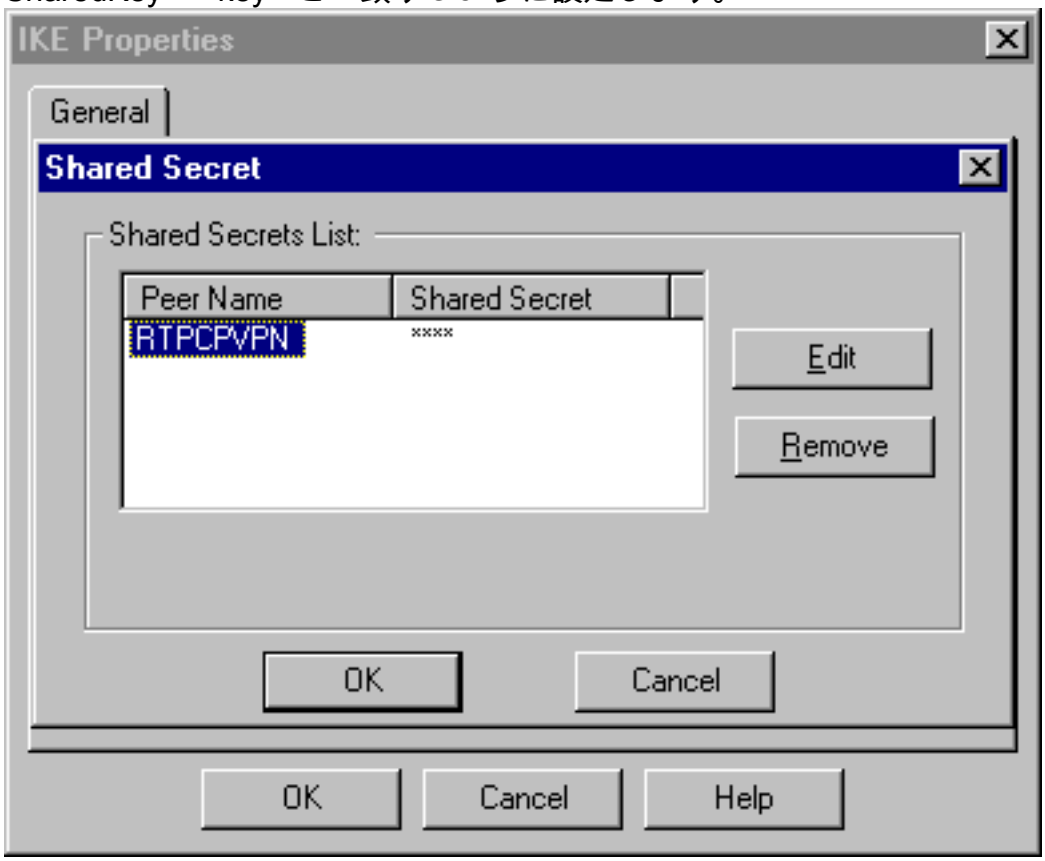


10. VPN コンセントレータ コマンドの **SHA_DES_G2 と一致するように IKE プロパティを [DES] 暗号化と [SHA1] ハッシュに変更します。注：**「G2」はDiffie-Hellmanグループ1または2を指します。テストでは、Checkpointが「G2」または「G1」を受け入れていることが判明しました。次の設定を変更します。[Aggressive Mode] をオフにします。[Supports Subnets] をオンにします。[Authentication Method] の [Pre-Shared Secret] をオンにします



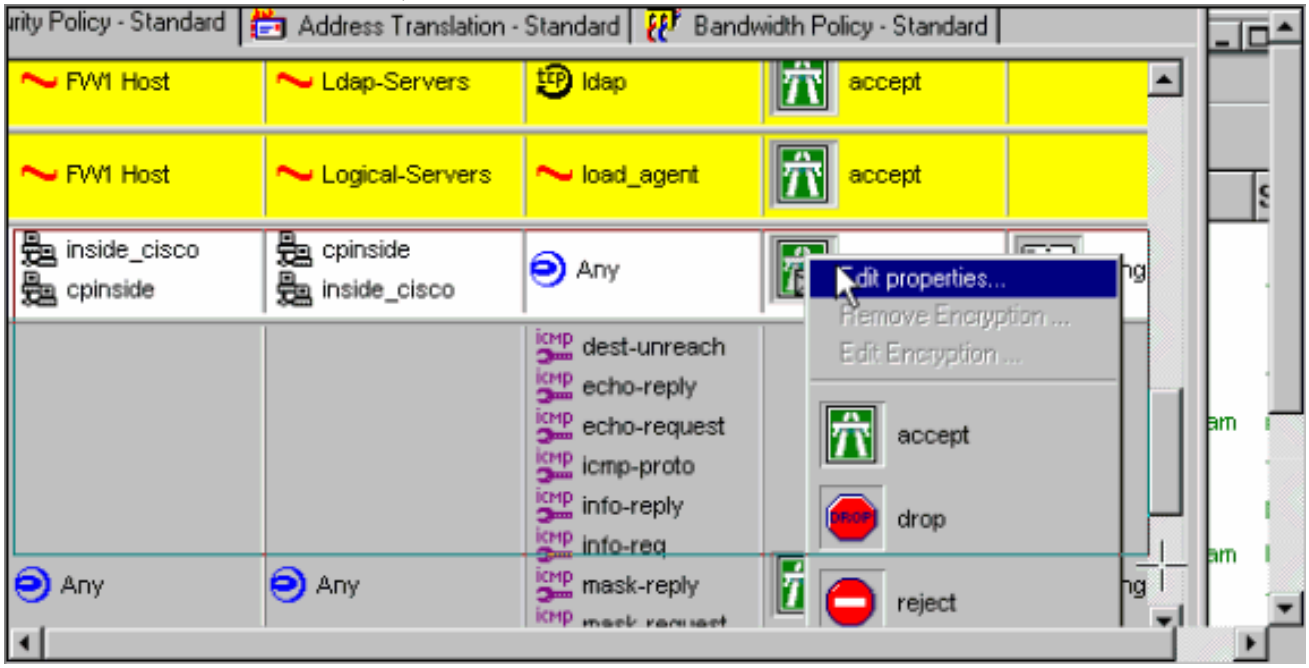
。

11. [Edit Secrets] をクリックし、事前共有キーを VPN コンセントレータ コマンドの SharedKey = <key> と一致するように設定します。

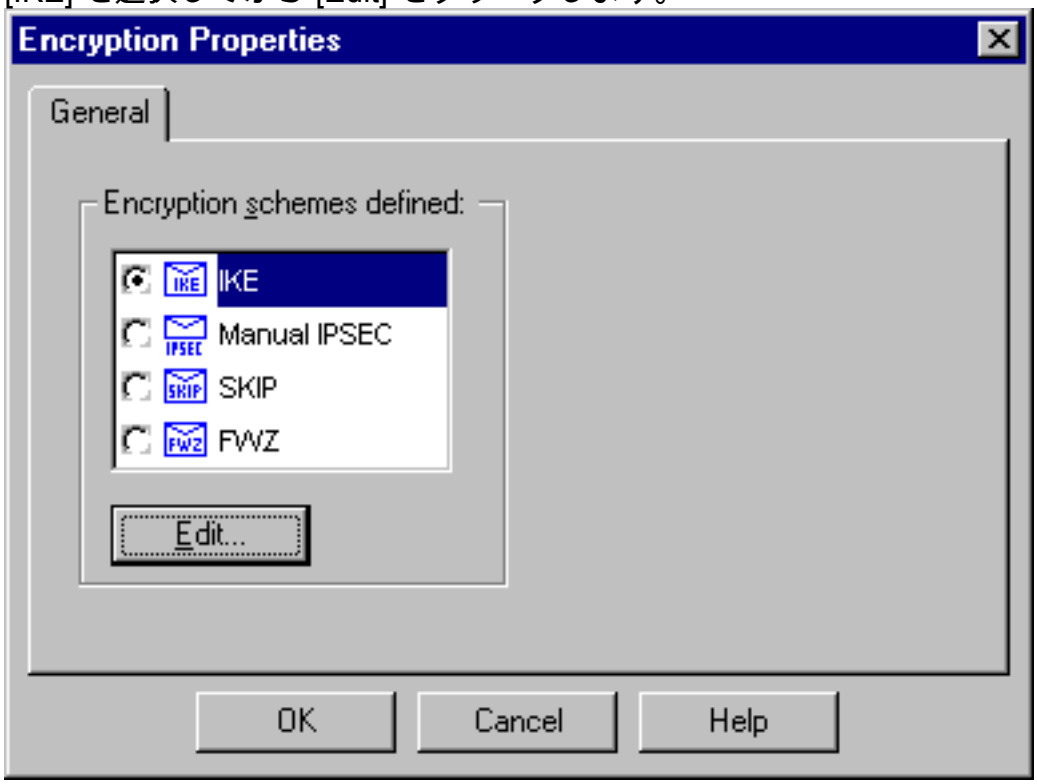


12. [Policy Editor] ウィンドウで、Source と Destination の両方に「inside_cisco」と「cpinside」（双方向）を設定したルールを挿入します。 **Service=Any**、**Action=Encrypt**、および **Track=Long** を設定します。

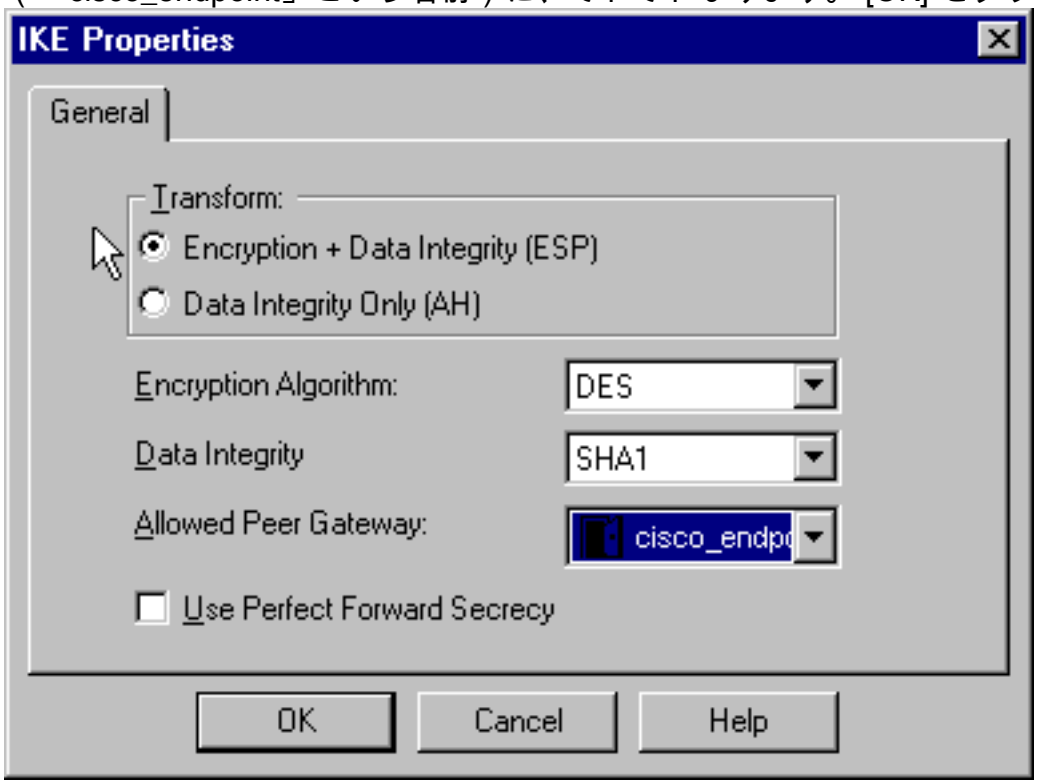
13. [Action] 見出しの下で、緑の [Encrypt] アイコンをクリックし、[Edit properties] を選択して暗号化ポリシーを設定します。



14. [IKE] を選択してから [Edit] をクリックします。



15. [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 コマンドの **Transform = esp(sha,des) 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 VPN コンセントレータ 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。



16. 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。

トラブルシュート

VPN 5000 コンセントレータのトラブルシューティング コマンド

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注：debug コマンドを使用する前に、**『debug コマンドの重要な情報』**を参照してください。

- **vpn trace dump all：すべての一致する VPN 接続の情報を表示します。時間、VPN 番号、ピアの実際の IP アドレス、どのスクリプトが実行されているかの情報、そしてエラーの場合はエラーが発生したソフトウェア コードのルーチンと回線番号が表示されます。**
- **show system log buffer：内部ログ バッファの内容を表示します。**
- **show vpn statistics：ユーザやパートナーの次の情報を表示します**（モジュラ モデルでは、ディスプレイには各モジュール スロットのセクションが含まれます。「デバッグのサンプル出力」を参照してください）。`Current ActiveIn NegotHigh WaterRunning TotalTunnel OKTunnel StartsTunnel Error`

- **show vpn statistics verbose：ISAKMP ネゴシエーション統計情報と、さらに多数のアクティブ接続の統計情報を表示します。**

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。

Checkpoint 4.1 Firewall のデバッグ

このデバッグは Microsoft Windows NT がインストールされている場合のものです。トラッキングは [Policy Editor] ウィンドウで Long 手順 12 を参照）、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を取得するには、次のコマンドを実行します。

```
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
```

次のコマンドを実行すると、チェックポイントでセキュリティ アソシエーション（SA）をクリアできます。

```
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_endpoint#vpn trac dump all
         4 seconds -- stepmngr trace enabled --
   new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing l2lp_init, (0 @ 0)
         38 seconds doing l2lp_do_negotiation, (0 @ 0)
   new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
```

```
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing l2lp_start_phase_2, (0 @ 0)
   new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_pkt_2_wait, (0 @ 0)
         39 seconds doing ihp2_process_pkt_2, (0 @ 0)
         39 seconds doing iph2_build_pkt_3, (0 @ 0)
         39 seconds doing iph2_config_SAs, (0 @ 0)
         39 seconds doing iph2_send_pkt_3, (0 @ 0)
         39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_open_tunnel, (0 @ 0)
         39 seconds doing l2lp_start_i_maint, (0 @ 0)
   new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)


cisco_endpoint#show vpn stat

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          ------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          ------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

cisco_endpoint#show vpn stat verb

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          ------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

Stats             VPN0:1
Wrapped               13
Unwrapped              9
BadEncap               0
BadAuth                0
BadEncrypt             0
rx IP                  9
rx IPX                 0
rx Other               0
tx IP                 13
tx IPX                 0
```

```
tx Other               0
IKE rekey              0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        4
Fastswitch packets in   0
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      1
Inserted cookie(R)      0
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        0
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0

IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          ------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

Stats
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
```

```
rx Other
tx IP
tx IPX
tx Other
IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in         0
Fastswitch packets in    3
No cookie found          0
Can't insert cookie      0
Inserted cookie(L)       0
Inserted cookie(R)       1
Cookie not inserted(L)   0
Cookie not inserted(R)   0
Cookie conn changed      0
Cookie already inserted  0
Deleted cookie(L)        0
Deleted cookie(R)        0
Cookie not deleted(L)    0
Cookie not deleted(R)    0
Forwarded to RP          0
Forwarded to IOP         3
Bad UDP checksum         0
Not fastswitched         0
Bad Initiator cookie     0
Bad Responder cookie     0
Has Responder cookie     0
No Responder cookie      0
No SA                    0
Bad find conn            0
Admin queue full         0
Priority queue full      0
Bad IKE packet           0
No memory                0
Bad Admin Put            0
IKE pkt dropped          0
No UDP PBuf              0
No Manager               0
Mgr w/ no cookie         0
Cookie Scavenge Add      1
Cookie Scavenge Rem      0
Cookie Scavenged         0
Cookie has mgr err       0
New conn limited         0
```

関連情報

- Cisco VPN 5000 シリーズ コンセントレータの販売終了のお知らせ
- 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