

チェックポイントNGとルータ間のIPSecトンネルの設定

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](#)

[Cisco 1751 VPN ルータの設定](#)

[Checkpoint NG の設定](#)

[確認](#)

[Cisco ルータの検証](#)

[Checkpoint NG の検証](#)

[トラブルシューティング](#)

[Cisco ルータ](#)

[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。

- ルータ内部のプライベートネットワーク 172.16.15.x
- CheckpointTM Next Generation (NG) 内のプライベートネットワーク 192.168.10.x

前提条件

要件

このドキュメントで説明している手順は、次の前提条件に基づいています。

- CheckpointTM NG の基本ポリシーが設定されている。
- すべてのアクセス、ネットワークアドレス変換 (NAT)、ルーティングの設定が行われている。
- ルータ内部と CheckpointTM NG 内部からインターネットへのトラフィックが流れている。

使用するコンポーネント

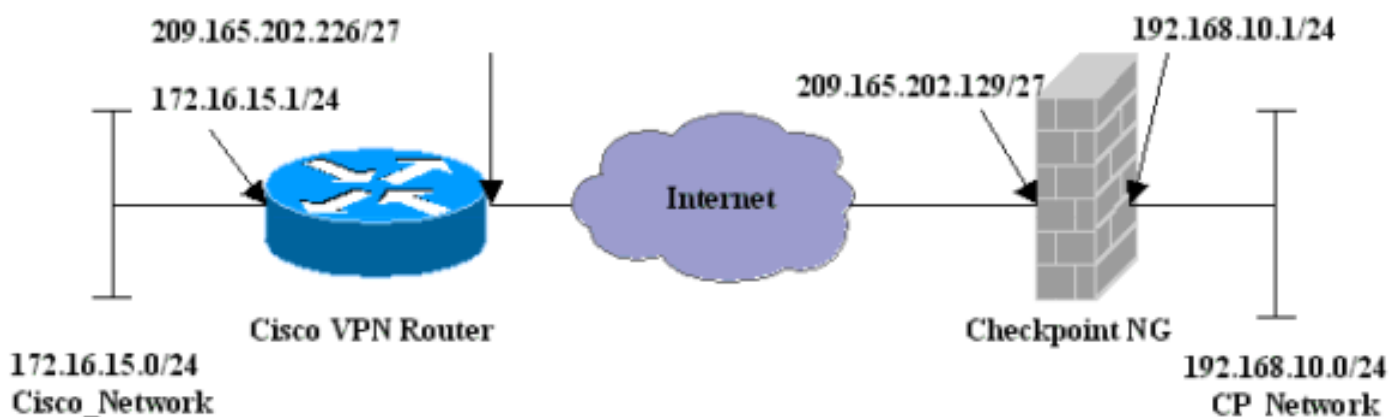
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco 1751 ルータ
- Cisco IOS®ソフトウェア(C1700-K9O3SY7-M)、バージョン12.2(8)T4、リリースソフトウェア(fc1)
- Checkpoint™ NG ビルド 50027

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

ドキュメントの表記法の詳細は、「[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。

Cisco 1751 VPN ルータの設定

Cisco VPN 1751 ルータ

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname svl-6
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip domain-lookup
ip audit notify log
ip audit po max-events 100
!--- Internet Key Exchange (IKE) configuration. crypto
isakmp policy 1
  encr 3des
```

```

hash md5
authentication pre-share
group 2
lifetime 1800
!--- IPsec configuration. crypto isakmp key aptrules
address 209.165.202.129
!
crypto ipsec transform-set aptset esp-3des esp-md5-hmac
!
crypto map aptmap 1 ipsec-isakmp
  set peer 209.165.202.129
  set transform-set aptset
  match address 110
!
interface Ethernet0/0
  ip address 209.165.202.226 255.255.255.224
  ip nat outside
  half-duplex
  crypto map aptmap
!
interface FastEthernet0/0
  ip address 172.16.15.1 255.255.255.0
  ip nat inside
  speed auto
!--- NAT configuration. ip nat inside source route-map
nonat interface Ethernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.225
no ip http server
ip pim bidir-enable
!--- Encryption match address access list. access-list
110 permit ip 172.16.15.0 0.0.0.255 192.168.10.0
0.0.0.255
!--- NAT access list. access-list 120 deny ip
172.16.15.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 120 permit ip 172.16.15.0 0.0.0.255 any
route-map nonat permit 10
  match ip address 120
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  password cisco
  login
end

```

Checkpoint NG の設定

The Checkpoint™ NG はオブジェクト指向の設定です。ネットワーク オブジェクトとルールを定義して、設定する VPN コンフィギュレーションに関するポリシーを作成します。その後、Checkpoint™ NG Policy Editor を使用してこのポリシーをインストールすると、Checkpoint™ NG 側の VPN コンフィギュレーションは完了します。

1. シスコ側のネットワークのサブネットと、Checkpoint™ NG 側のネットワークのサブネットを、ネットワーク オブジェクトとして作成します。これが暗号化されます。オブジェクトを作成するには、[Manage] > [Network Objects] の順に選択し、続いて [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。これらの例は、CP_Network および Cisco_Network という名前のオブジェクトの設定を示しています。

Network Properties - CP_Network

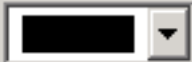
General NAT

Name: CP_Network

IP Address: 192.168.10.0

Net Mask: 255.255.255.0

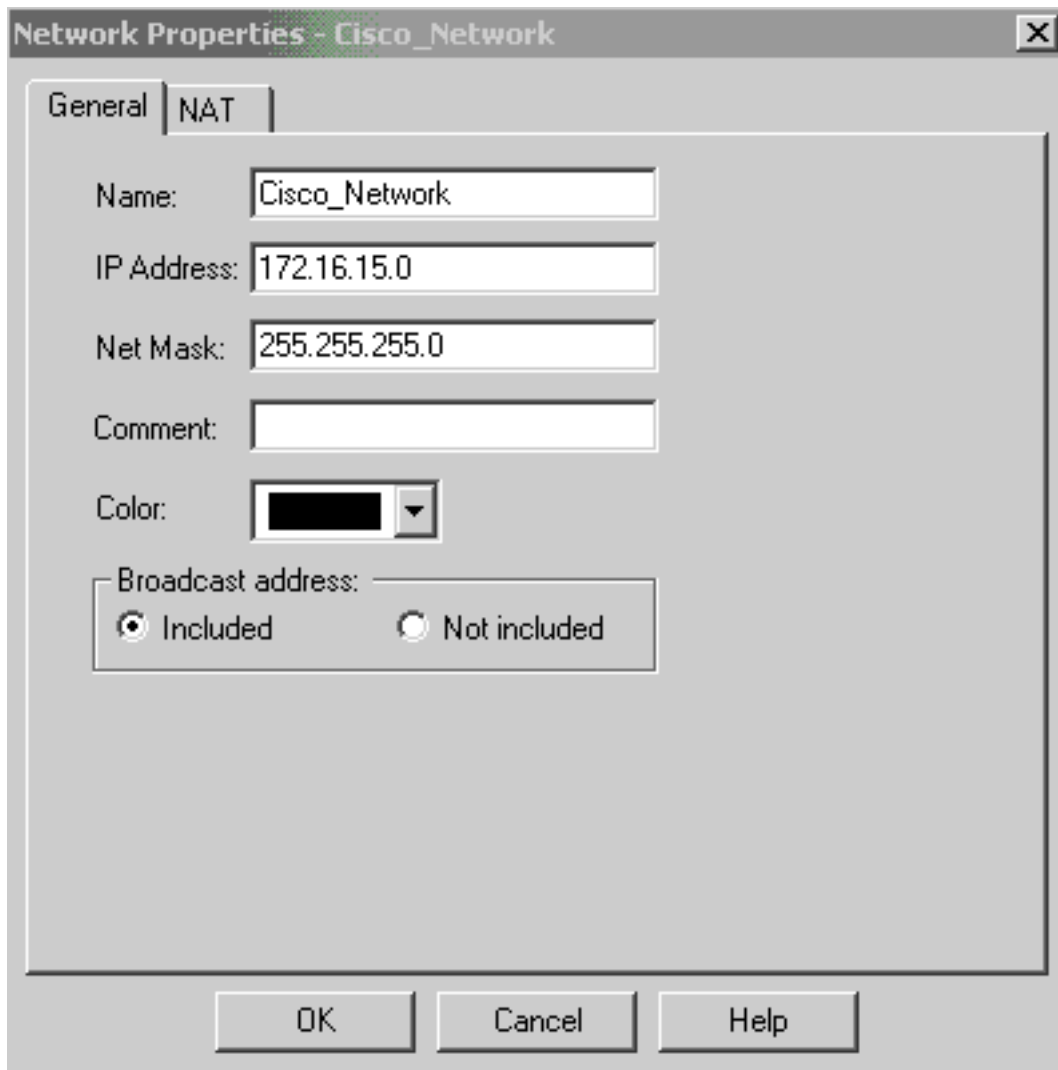
Comment:

Color: 

Broadcast address:

Included Not included

OK Cancel Help



2. Cisco_Router オブジェクトと Checkpoint_NG オブジェクトをワークステーション オブジェクトとして作成します。これらは VPN デバイスです。オブジェクトを作成するには、[Manage] > [Network Objects] の順に選択し、続いて [New] > [Workstation] を選択します。CheckpointTM NG の初期設定の際に作成した CheckpointTM 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 [Gateway] および [Interoperable VPN Device] として設定するオプションを選択します。これらの例は、chef および Cisco_Router という名前のオブジェクトの設定を示しています。

General

Topology

NAT

VPN

Authentication

Management

+ Advanced

General

Name: chef

IP Address: 209.165.202.129

Comment: CP_Server

Color: Type: Host Gateway

Check Point Products

 Check Point products installed: Version NG

- 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)

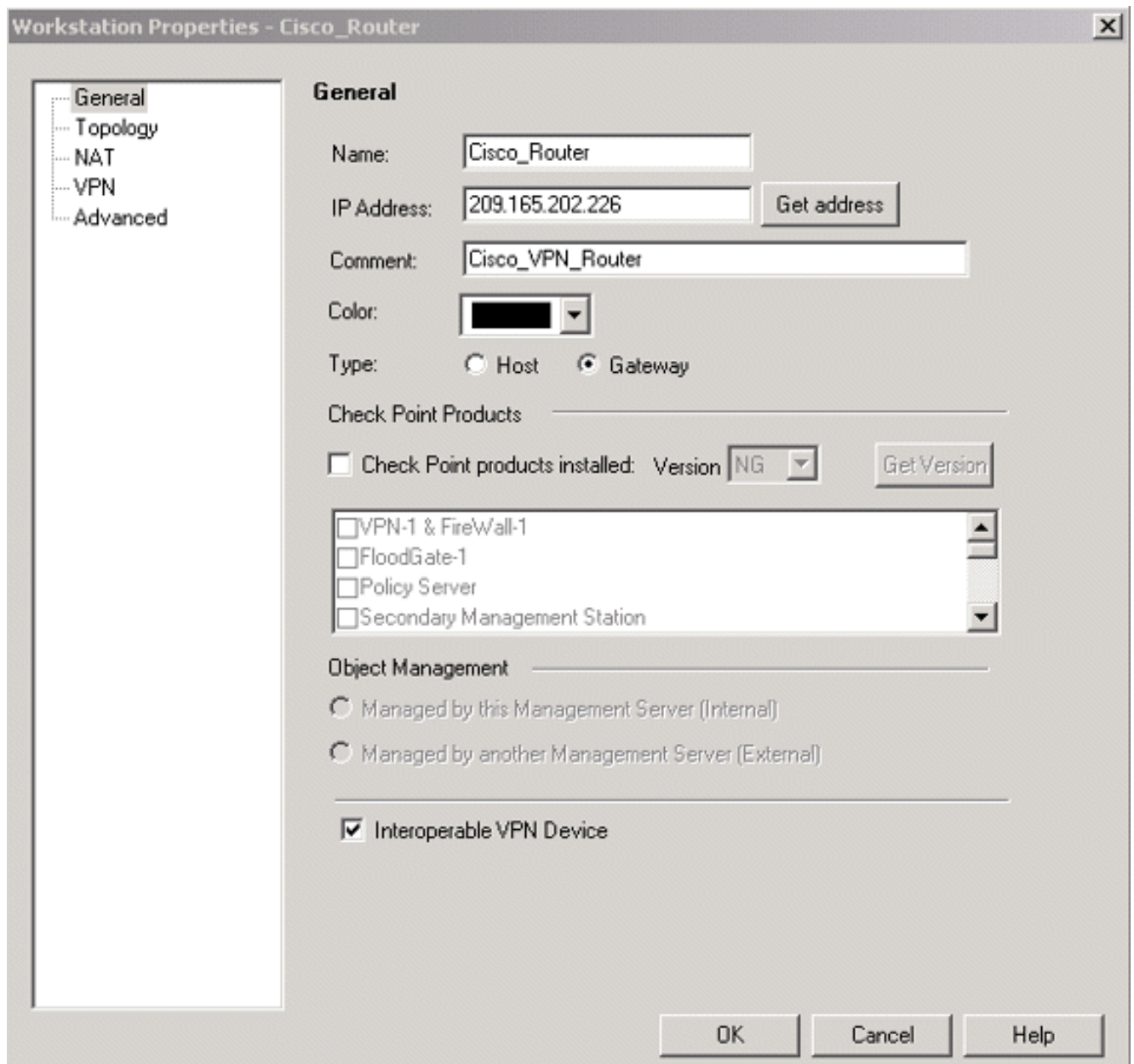
Secure Internal Communication

 DN: cn=cp_mgmt,o=chef.6h9tua Interoperable VPN Device

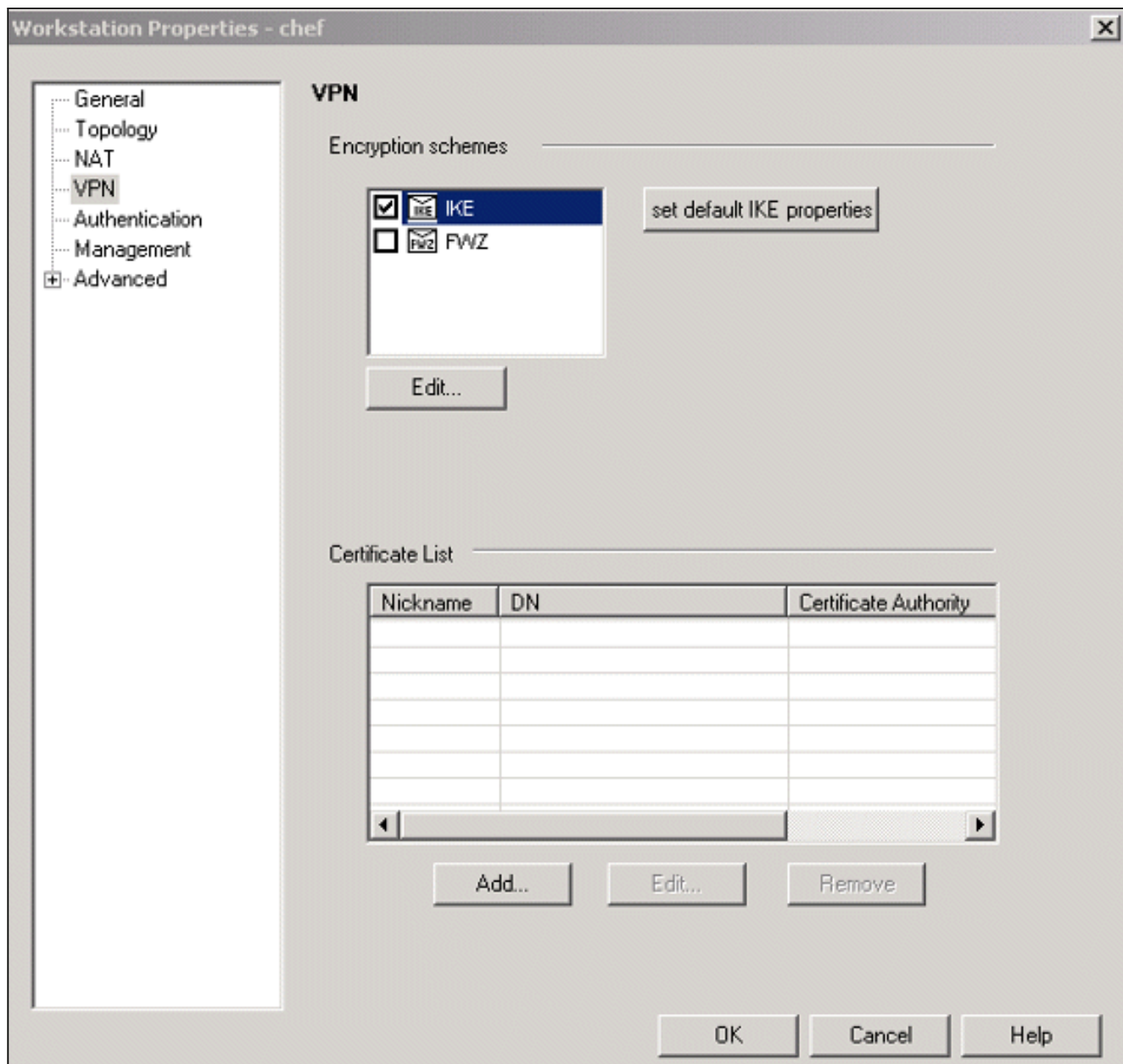
OK

Cancel

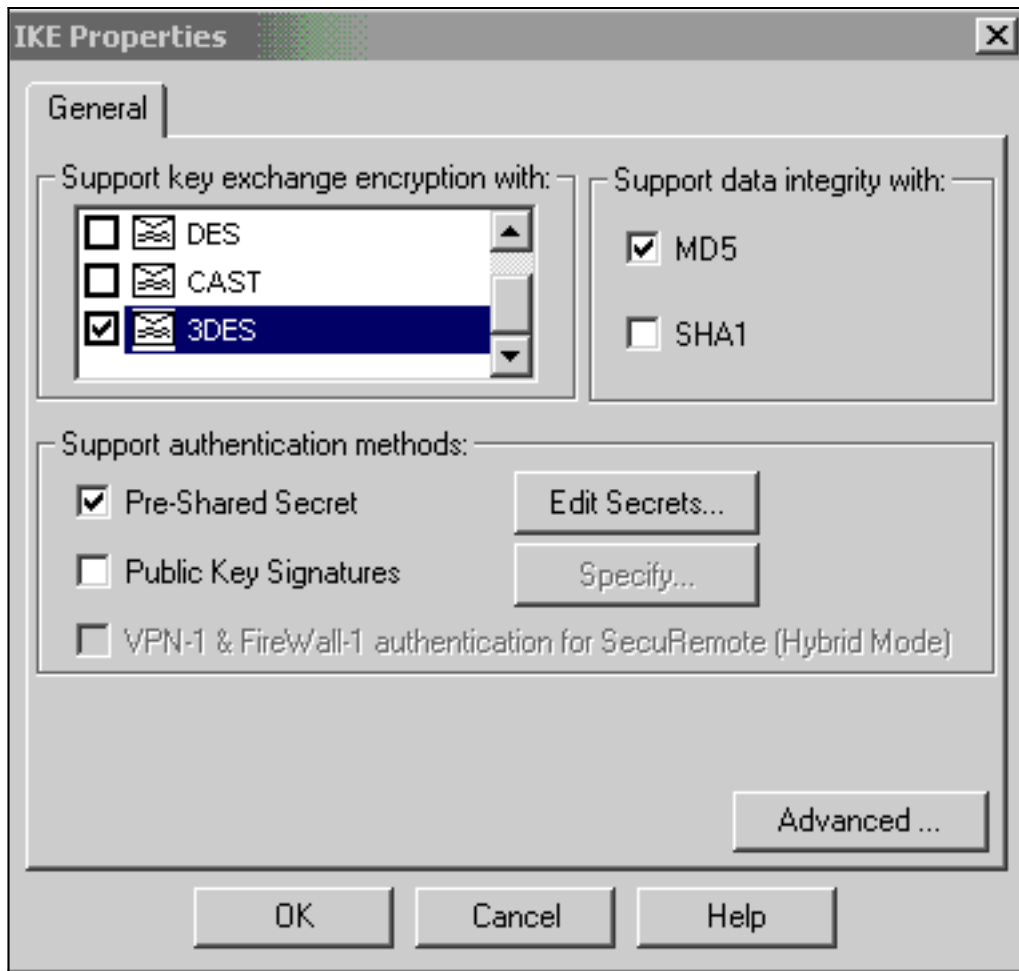
Help



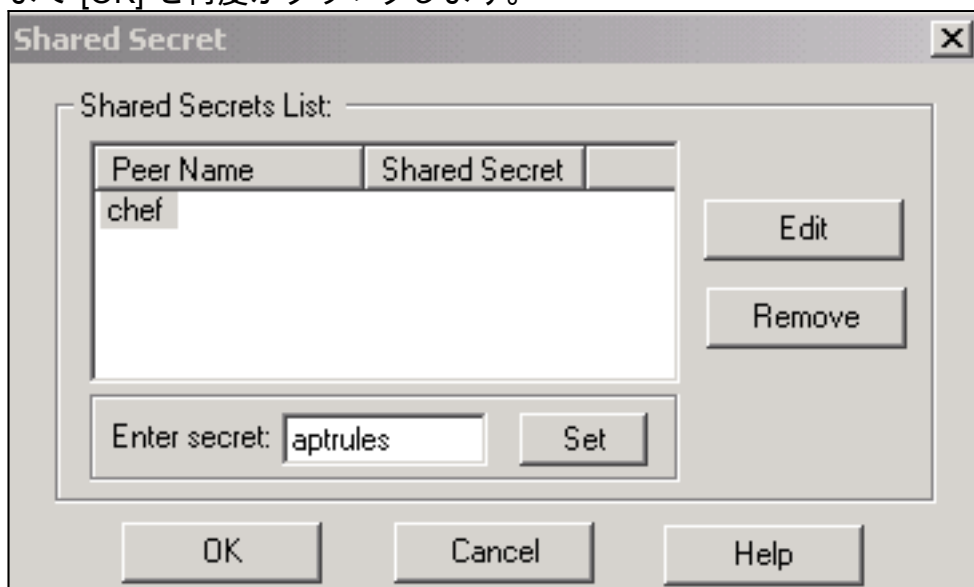
3. [VPN] タブで [IKE] を設定し、[Edit] をクリックします。



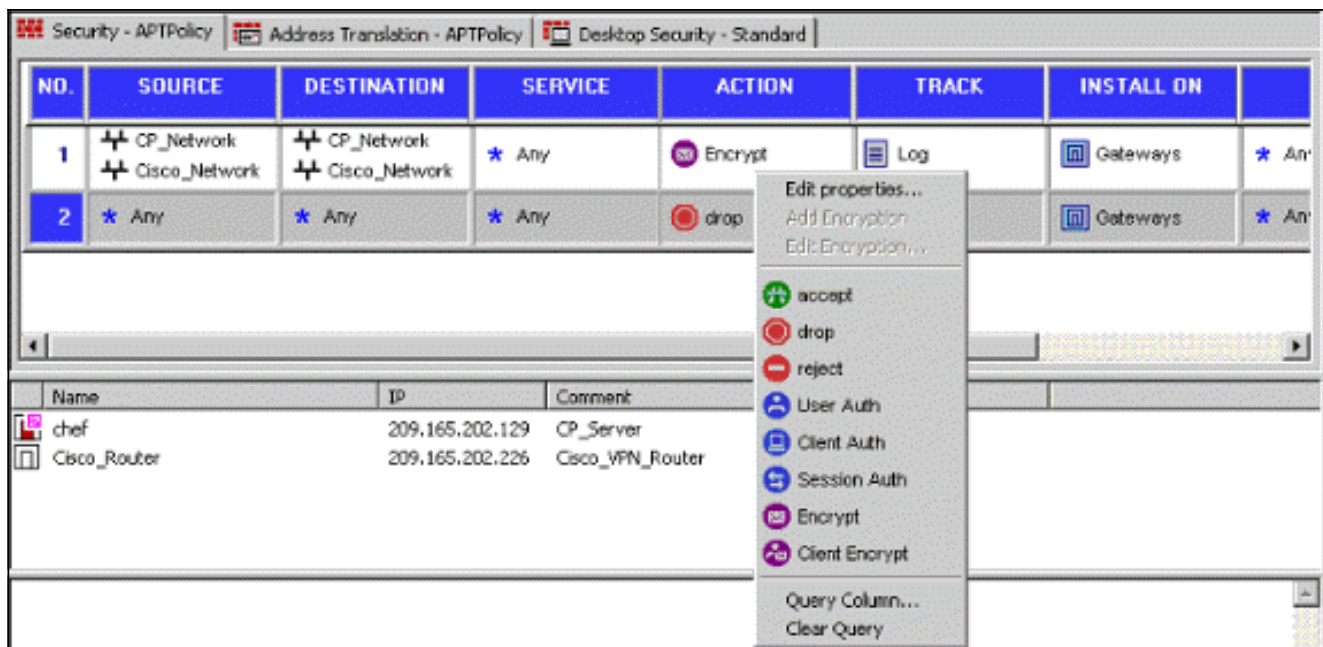
4. キー交換ポリシーを設定して、[Edit Secrets] をクリックします。



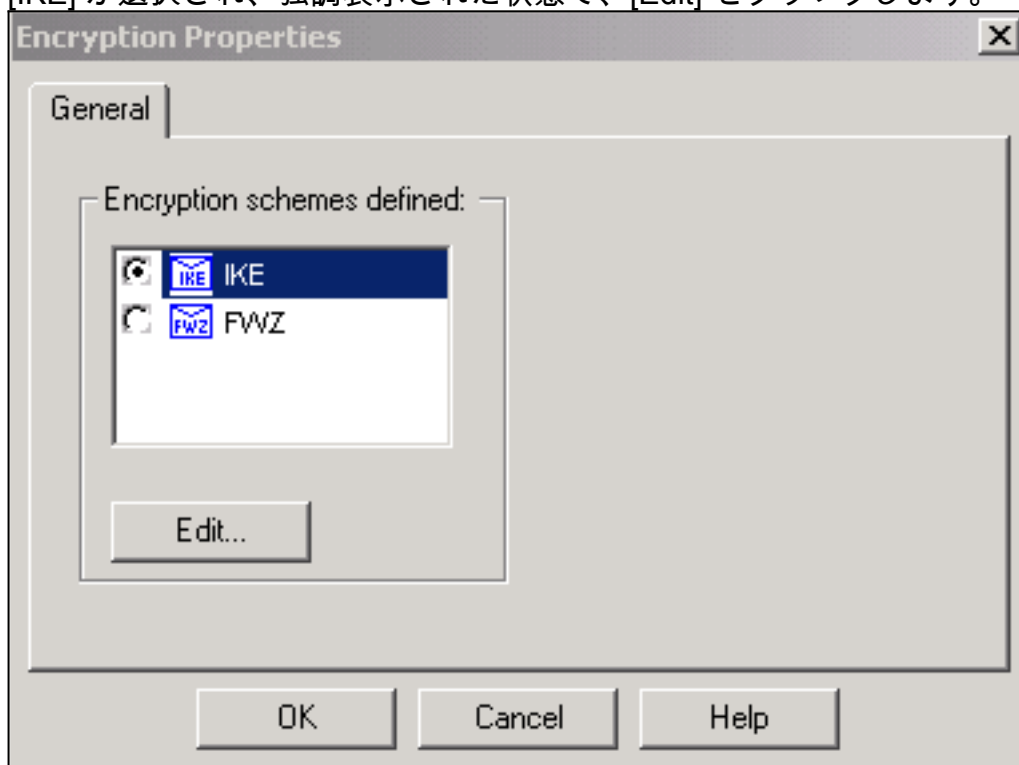
5. 使用する事前共有キーを設定し、コンフィギュレーション ウィンドウが表示されなくなるまで [OK] を何度かクリックします。



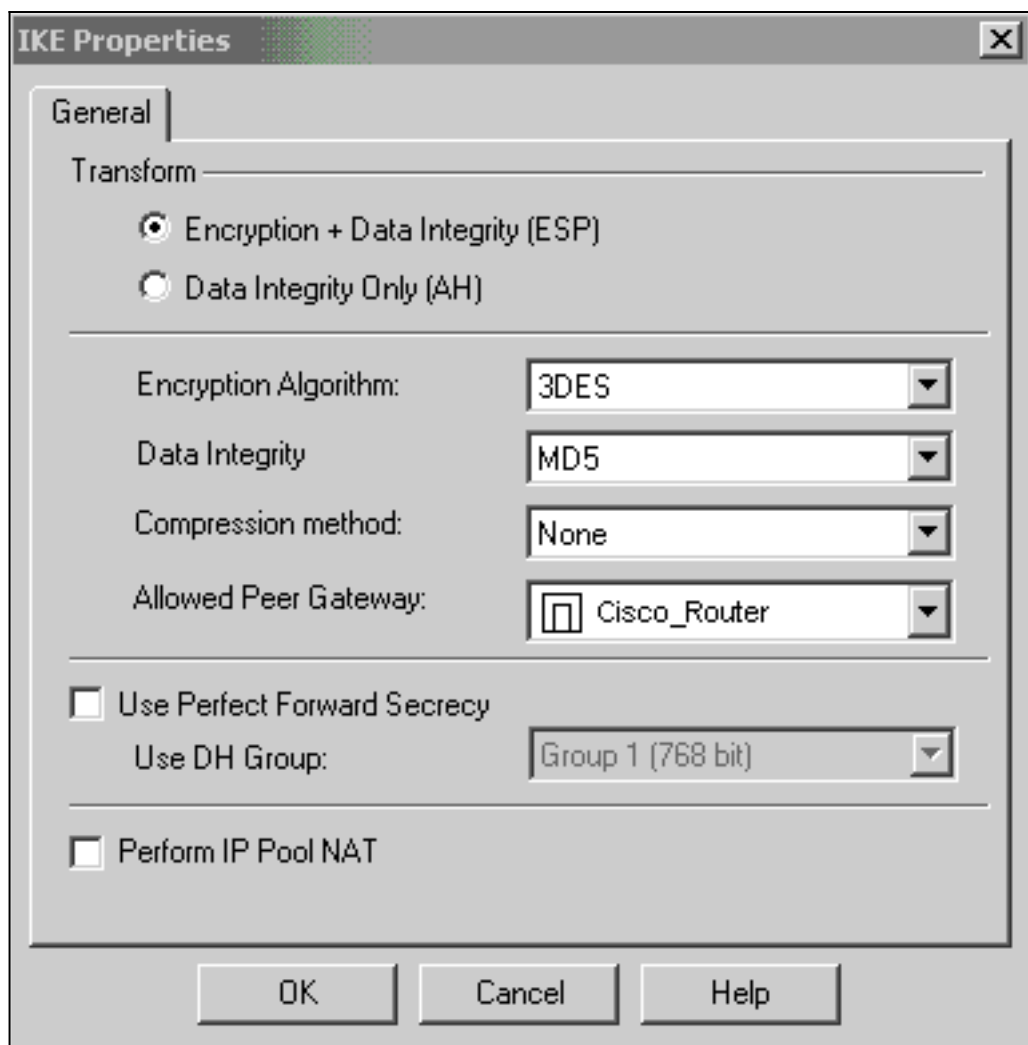
6. [Rules] > [Add Rules] > [Top] を選択して、ポリシーの暗号化ルールを設定します。先頭にあるルールは、暗号化をバイパスする可能性がある他のルールより前に、一番最初に実行されるルールです。次に示すように、Source と Destination を設定して、CP_Network と Cisco_Network を含めます。ルールの [Encrypt Action] セクションを追加したら、[Action] を右クリックして、[Edit Properties] を選択します。



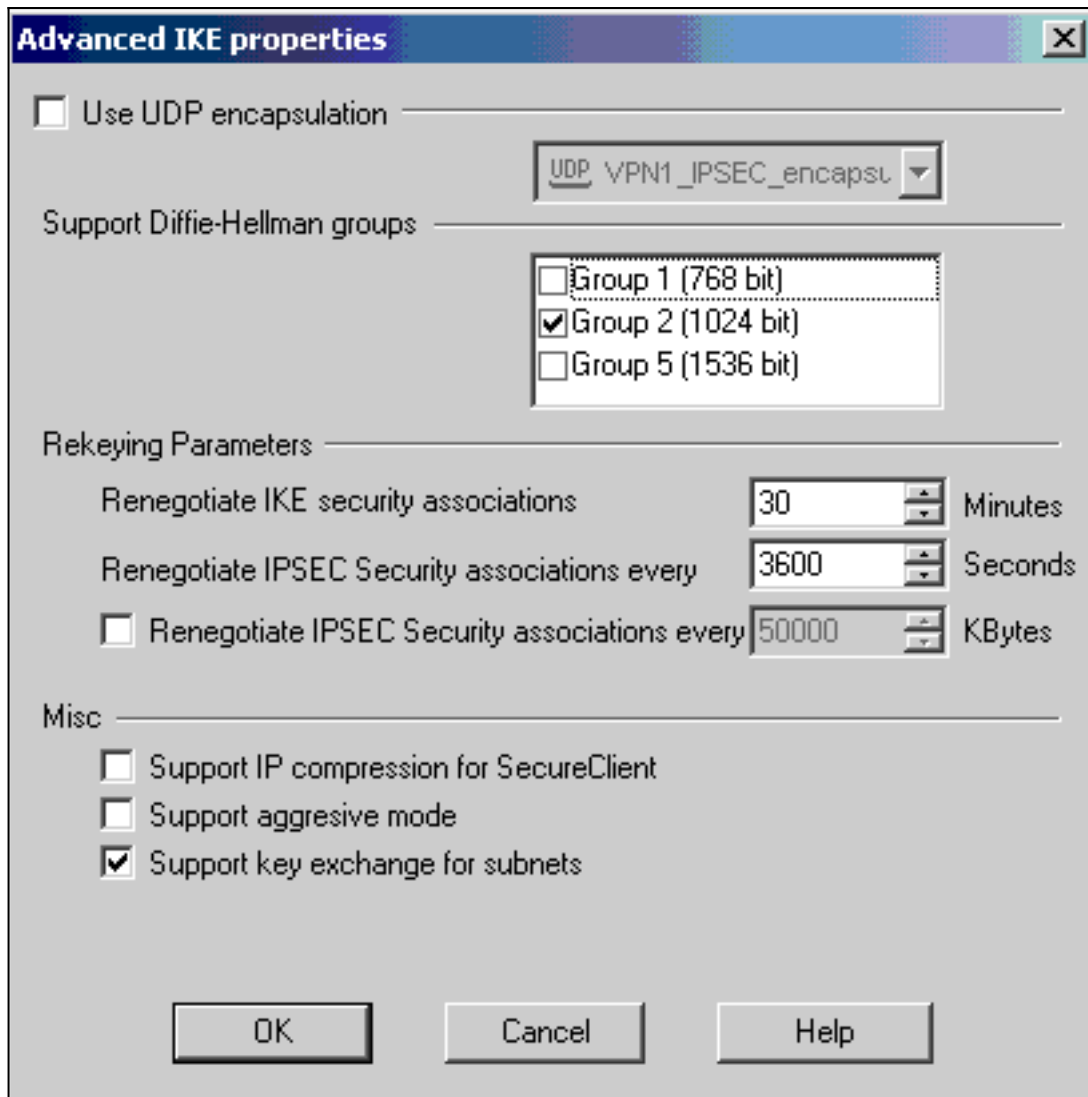
7. [IKE] が選択され、強調表示された状態で、[Edit] をクリックします。



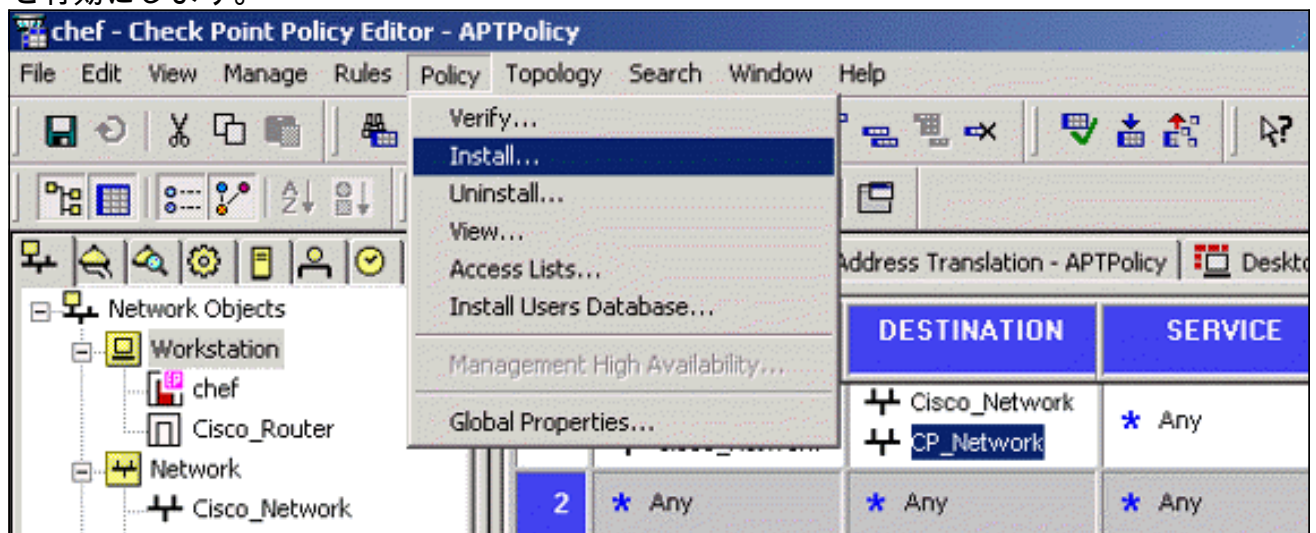
8. IKE の設定を確認します。



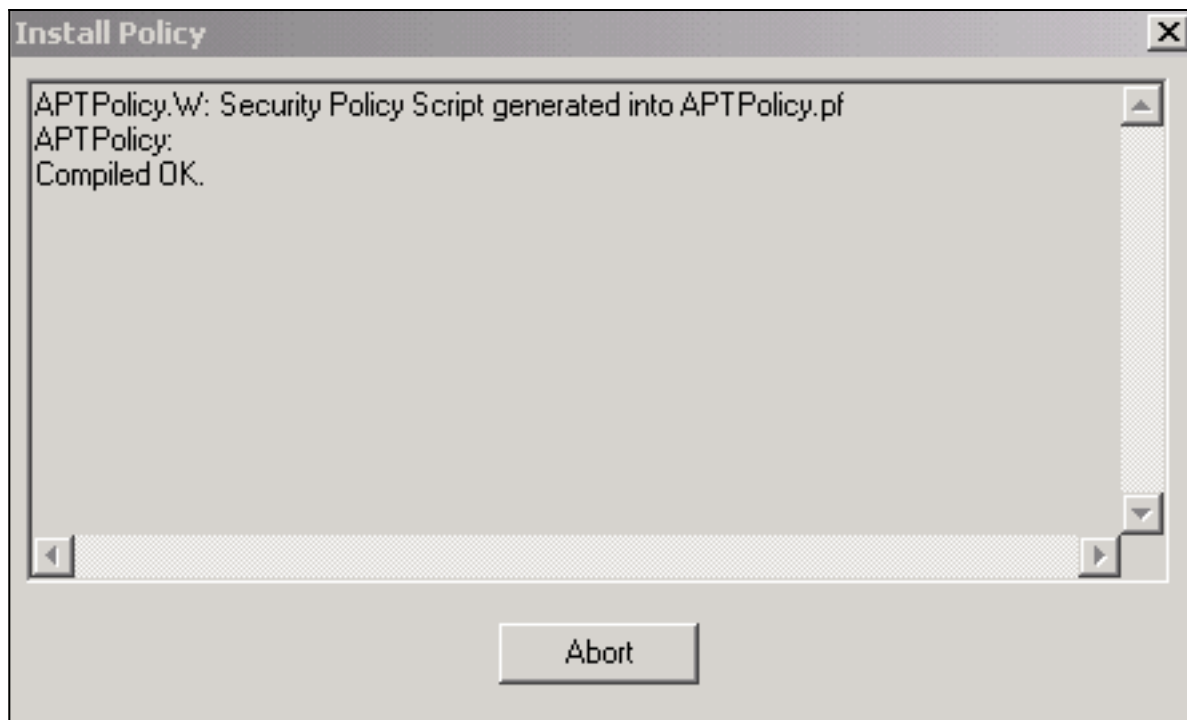
9. Cisco デバイスと他の IPSec デバイスとの間で VPN を実行する場合の主な問題の 1 つは、キー交換の再ネゴシエーションです。Cisco ルータでの IKE 交換の設定が、CheckpointTM NG での設定と正確に一致するようにします。注：このパラメータの実際の値は、特定の企業セキュリティポリシーによって異なります。この例では、[ルータでの IKE の設定は、lifetime 1800 コマンドによって 30 分に設定されています](#)。CheckpointTM NG でも同じ値を設定する必要があります。この値を CheckpointTM NG に設定するには、[Manage Network Object] を選択し、次に CheckpointTM NG オブジェクトを選択して [Edit] をクリックします。次に [VPN] を選択して IKE を編集します。[Advance] を選択して、Rekeying Parameters を設定します。CheckpointTM NG ネットワーク オブジェクトのキー交換を設定した後、Cisco_Router ネットワーク オブジェクトのキー交換の再ネゴシエーションに対しても同じ設定を行います。注：ルータで設定されている Diffie-Hellman グループと一致するように、正しい Diffie-Hellman グループが選択されていることを確認してください。



10. これでポリシー設定は完了です。ポリシーを保存して、[Policy] > [Install] を選択してこれを有効にします。

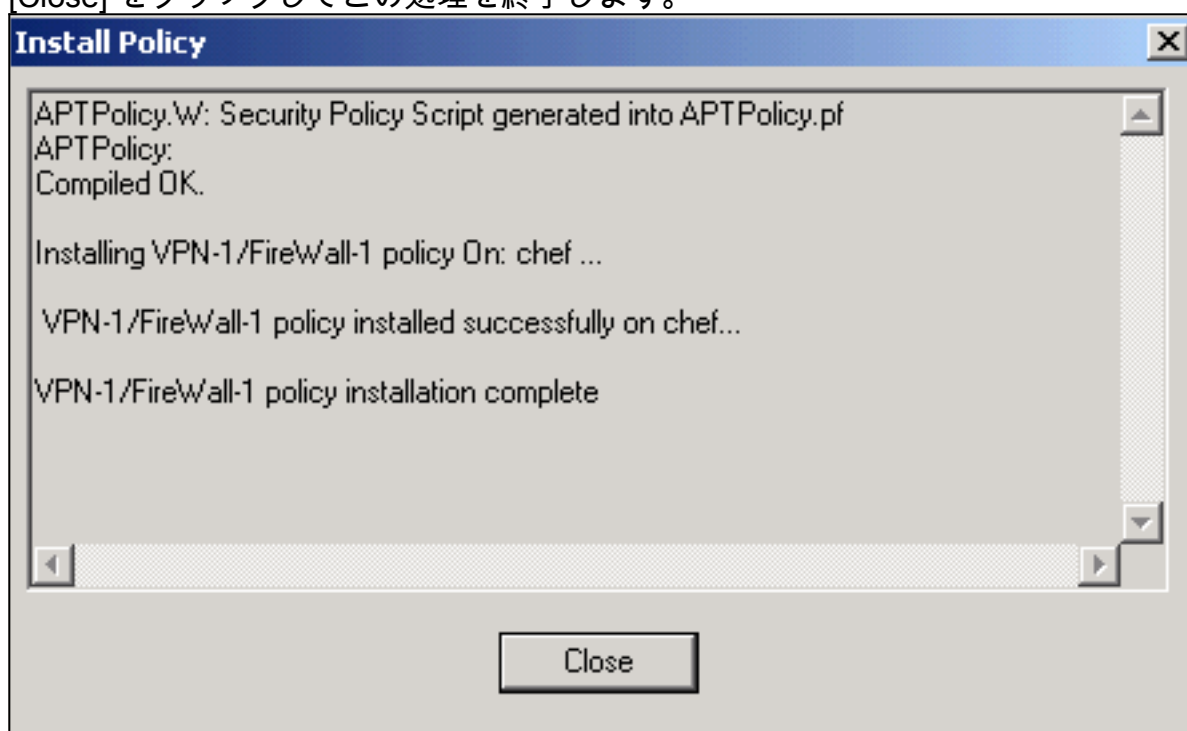


ポリシーがコンパイルされるときには、インストレーション ウィンドウに進捗状態が表示されます。



インス

トレーション ウィンドウに、ポリシーのインストールが完了したことが表示されたら、[Close] をクリックしてこの処理を終了します。



確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

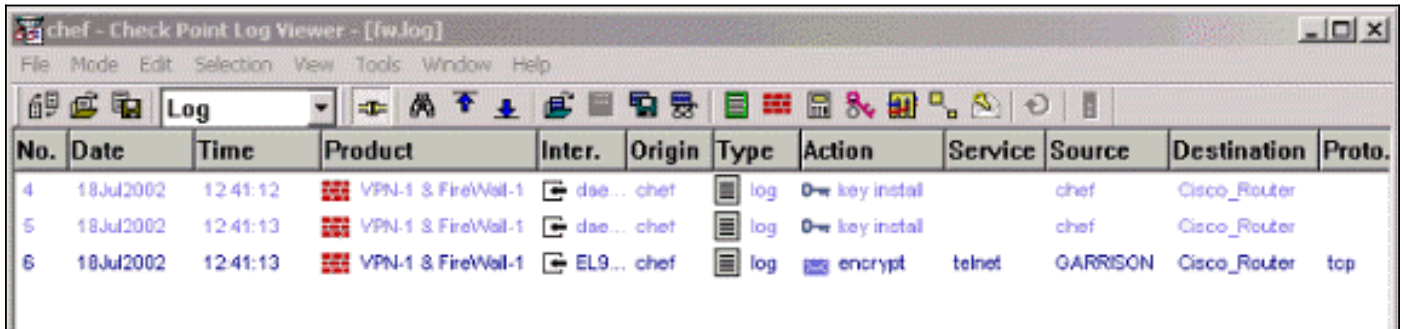
Cisco ルータの検証

一部の show コマンドは [アウトプット インタープリタ ツール](#) によってサポートされています ([登録ユーザ専用](#))。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- show crypto isakmp sa : ピア上の現在の IKE セキュリティ アソシエーション (SA) をすべて表示します。
- show crypto ipsec sa : 現在の SA で使用されている設定を表示します。

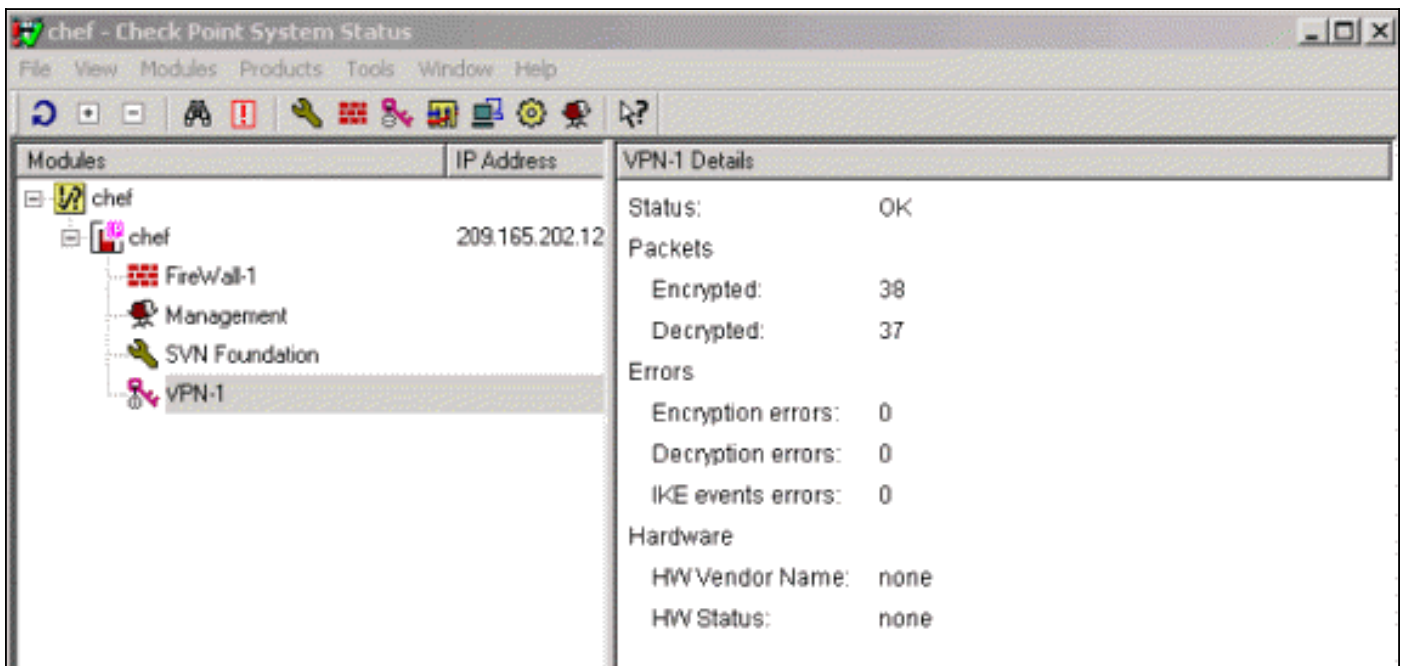
Checkpoint NG の検証

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



No.	Date	Time	Product	Inter.	Origin	Type	Action	Service	Source	Destination	Proto.
4	18Jul2002	12:41:12	VPN-1 & FireWall-1	dae...	chef	log	key instal		chef	Cisco_Router	
5	18Jul2002	12:41:13	VPN-1 & FireWall-1	dae...	chef	log	key instal		chef	Cisco_Router	
6	18Jul2002	12:41:13	VPN-1 & FireWall-1	EL9...	chef	log	encrypt	telnet	GARRISON	Cisco_Router	tcp

システムのステータスを表示するには、[Window] > [System Status] の順に選択します。



Modules	IP Address	VPN-1 Details
chef		Status: OK
chef	209.165.202.12	Packets
FireWall-1		Encrypted: 38
Management		Decrypted: 37
SVN Foundation		Errors
VPN-1		Encryption errors: 0
		Decryption errors: 0
		IKE events errors: 0
		Hardware
		HW Vendor Name: none
		HW Status: none

トラブルシューティング

Cisco ルータ

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。

このほかのトラブルシューティングについては、「[IP Security のトラブルシューティング - debug コマンドの理解と使用](#)」を参照してください。

注 : debugコマンドを発行する前に、「[debugコマンドの重要な情報](#)」を参照してください。

- debug crypto engine : 暗号化と復号化を行う暗号化エンジンに関するデバッグ メッセージを表示します。

- **debug crypto isakmp** : IKE イベントに関するメッセージを表示します。
- **debug crypto ipsec** : IPsec イベントを表示します。
- **clear crypto isakmp** : **すべてのアクティブな IKE 接続をクリアします。**
- **clear crypto sa** : **すべての IPSec SA をクリアします。**

正常な debug ログの出力

```

18:05:32: ISAKMP (0:0): received packet from
      209.165.202.129 (N) NEW SA
18:05:32: ISAKMP: local port 500, remote port 500
18:05:32: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
      IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
18:05:32: ISAKMP (0:1): processing SA payload. message ID = 0
18:05:32: ISAKMP (0:1): processing vendor id payload
18:05:32: ISAKMP (0:1): vendor ID seems Unity/DPD
      but bad major
18:05:32: ISAKMP (0:1): found peer pre-shared key
      matching 209.165.202.129
18:05:32: ISAKMP (0:1): Checking ISAKMP transform 1
      against priority 1 policy
18:05:32: ISAKMP: encryption 3DES-CBC
18:05:32: ISAKMP: hash MD5
18:05:32: ISAKMP: auth pre-share
18:05:32: ISAKMP: default group 2
18:05:32: ISAKMP: life type in seconds
18:05:32: ISAKMP: life duration (VPI) of 0x0 0x0 0x7 0x8
18:05:32: ISAKMP (0:1): atts are acceptable. Next payload is 0
18:05:33: ISAKMP (0:1): processing vendor id payload
18:05:33: ISAKMP (0:1): vendor ID seems Unity/DPD but bad major
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
      IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
      MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
      IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
      MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
      IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): processing KE payload.
      message ID = 0
18:05:33: ISAKMP (0:1): processing NONCE payload.
      message ID = 0
18:05:33: ISAKMP (0:1): found peer pre-shared key
      matching 209.165.202.129
18:05:33: ISAKMP (0:1): SKEYID state generated
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
      IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
      MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
      IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
      MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
      IKE_MM_EXCH

```

Old State = IKE_R_MM4 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): processing ID payload.
message ID = 0
18:05:33: ISAKMP (0:1): processing HASH payload.
message ID = 0
18:05:33: ISAKMP (0:1): SA has been authenticated
with 209.165.202.129
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
18:05:33: ISAKMP (1): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
18:05:33: ISAKMP (1): Total payload length: 12
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129
(R) QM_IDLE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
QM_IDLE
18:05:33: ISAKMP (0:1): processing HASH payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): processing SA payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): Checking IPsec proposal 1
18:05:33: ISAKMP: transform 1, ESP_3DES
18:05:33: ISAKMP: attributes in transform:
18:05:33: ISAKMP: SA life type in seconds
18:05:33: ISAKMP: SA life duration (VPI) of 0x0 0x0 0xE 0x10
18:05:33: ISAKMP: authenticator is HMAC-MD5
18:05:33: ISAKMP: encaps is 1
18:05:33: ISAKMP (0:1): atts are acceptable.
18:05:33: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 209.165.202.226, remote= 209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
18:05:33: ISAKMP (0:1): processing NONCE payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): asking for 1 spis from ipsec
18:05:33: ISAKMP (0:1): Node -1335371103,
Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(spi_response): getting spi 2147492563 for SA
from 209.165.202.226 to 209.165.202.129 for prot 3
18:05:33: ISAKMP: received ke message (2/1)
18:05:33: ISAKMP (0:1): sending packet to


```
209.165.202.129 (R) QM_IDLE
18:05:33: ISAKMP (0:1): Node -1335371103,
Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
18:05:33: ISAKMP (0:1): received packet
from 209.165.202.129 (R) QM_IDLE
18:05:33: ISAKMP (0:1): Creating IPsec SAs
18:05:33: inbound SA from 209.165.202.129 to 209.165.202.226
(proxy 192.168.10.0 to 172.16.15.0)
18:05:33: has spi 0x800022D3 and conn_id 200 and flags 4
18:05:33: lifetime of 3600 seconds
18:05:33: outbound SA from 209.165.202.226 to 209.165.202.129
(proxy 172.16.15.0 to 192.168.10.0 )
18:05:33: has spi -2006413528 and conn_id 201 and flags C
18:05:33: lifetime of 3600 seconds
18:05:33: ISAKMP (0:1): deleting node -1335371103 error
FALSE reason "quick mode done (await())"
18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MSG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 209.165.202.226,
remote=209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 3600s and 0kb,
spi= 0x800022D3(2147492563), conn_id= 200, keysize= 0,
flags= 0x4
18:05:33: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 209.165.202.226,
remote=209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 3600s and 0kb,

spi= 0x88688F28(2288553768), conn_id= 201, keysize= 0,
flags= 0xC
18:05:33: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.165.202.226, sa_prot= 50,
sa_spi= 0x800022D3(2147492563),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 200
18:05:33: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.165.202.129, sa_prot= 50,
sa_spi= 0x88688F28(2288553768),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 201
18:05:34: ISAKMP (0:1): received packet
from 209.165.202.129 (R) QM_IDLE
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate
of a previous packet.
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
node marked dead -1335371103
18:05:34: ISAKMP (0:1): received packet
from 209.165.202.129 (R) QM_IDLE
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate
of a previous packet.
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
node marked dead -1335371103
```

```

svl-6#show crypto isakmp sa
dst src state conn-id slot
209.165.202.226 209.165.202.129 QM_IDLE 1 0

svl-6#show crypto ipsec sa
interface: Ethernet0/0
Crypto map tag: aptmap, local addr. 209.165.202.226
local ident (addr/mask/prot/port): (172.16.15.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
current_peer: 209.165.202.129
PERMIT, flags={origin_is_acl,}
#pkts encaps: 21, #pkts encrypt: 21, #pkts digest 21
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 209.165.202.226, remote crypto endpt.: 209.165.202.129
path mtu 1500, media mtu 1500
current outbound spi: 88688F28
inbound esp sas:
spi: 0x800022D3(2147492563)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 200, flow_id: 1, crypto map: aptmap
sa timing: remaining key lifetime (k/sec): (4607997/3559)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x88688F28(2288553768)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 201, flow_id: 2, crypto map: aptmap
sa timing: remaining key lifetime (k/sec): (4607997/3550)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:

svl-6#show crypto engine conn act
ID Interface IP- Address State Algorithm Encrypt Decrypt
1 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 0 0
200 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 0 24
201 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 21 0

```

関連情報

- [IPSec に関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)