

# IPSec トンネルの設定 - Checkpoint 4.1 Firewall への Cisco ルータ-

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[ネットワーク集約](#)

[チェックポイント](#)

[デバッグの出力例](#)

[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。この2つのプライベート ネットワークは、Cisco ルータ内の 192.168.1.x プライベート ネットワークと Checkpoint Firewall 内部の 10.32.50.x プライベート ネットワークです。

## 前提条件

### 要件

この設定 例はインターネット ( 172.18.124.x ネットワークによってここに表される ) フローにルータおよび内部の中から設定を開始する前にとトラフィック Checkpoint 仮定します。

### 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くものです。

- Cisco 3600 ルータ
- Cisco IOS® ソフトウェア ( C3640-JO3S56I-M )、リリース 12.1(5)T、リリースソフトウェア

ア ( fc1 )

- Checkpoint Firewall 4.1

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たものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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、次のネットワーク構成を使用しています。

## 設定

このドキュメントでは、次の設定を使用します。

- [ルータの設定](#)
- [チェックポイントファイアウォール 設定](#)

## ルータの設定

### Cisco 3600 ルータ 設定

```
Current configuration : 1608 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) configuration crypto
```

```
isakmp policy 1 authentication pre-share crypto isakmp
key ciscorules address 172.18.124.157 !!-- IPsec
configuration crypto ipsec transform-set rtpset esp-des
esp-sha-hmac ! crypto map rtp 1 ipsec-isakmp set peer
172.18.124.157 set transform-set rtpset match address
115 ! call rsvp-sync cns event-service server !
controller T1 1/0 ! controller T1 1/1 ! interface
Ethernet0/0 ip address 172.18.124.35 255.255.255.240 ip
nat outside no ip mroute-cache half-duplex crypto map
rtp ! interface Ethernet0/1 ip address 192.168.1.1
255.255.255.0 ip nat inside half-duplex ! interface
FastEthernet1/0 no ip address shutdown duplex auto speed
auto ! ip kerberos source-interface any ip nat pool
INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240 ip nat inside source route-map nonat
pool INTERNET ip classless ip route 0.0.0.0 0.0.0.0
172.18.124.34 no ip http server ! access-list 101 deny
ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255 access-
list 101 permit ip 192.168.1.0 0.0.0.255 any access-list
115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any route-
map nonat permit 10 match ip address 101 ! dial-peer cor
custom ! line con 0 transport input none line aux 0 line
vty 0 4 login ! end
```

## チェックポイントファイアウォール設定

チェックポイントファイアウォールを設定するためにこれらのステップを完了して下さい。

1. IKE および IPSec デフォルト ライフタイムがベンダーの間で異なるので、チェックポイントライフタイムを Cisco デフォルトと一致するために設定するために Properties > Encryption の順に選択して下さい。Cisco デフォルト IKE ライフタイムは 86400 秒 (= 1440 分) であり、これらのコマンドによって修正することができます: `crypto isakmp policy #ライフタイム#` 設定可能な Cisco IKE ライフタイムは 60-86400 秒からです。Cisco デフォルト IPSec ライフタイムは 3600 秒であり、`crypto ipsec security-association lifetime seconds -` コマンドによって修正することができます。Cisco IPsec の 設定可能なライフタイムは 120-86400 秒からです。
2. Checkpoint の後ろの内部ネットワークのためのオブジェクトを ( 「cpinside」と呼ばれる ) 設定するために Manage > Network objects > New ( or Edit ) > Network の順に選択して下さい。これは Cisco `access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255` コマンドの宛先 ( セカンド ) ネットワークと一致するはずです。[Location] の [Internal] を選択します。
3. RTPCPVPN Checkpoint ( ゲートウェイ ) エンドポイントのためのオブジェクトをことピア `172.18.124.157` 一定コマンドの Cisco ルータ ポイント編集するために Manage > Network objects > Edit の順に選択して下さい。[Location] の [Internal] を選択します。Type で Gateway を選択します。インストールされるモジュールの下で VPN-1 & FireWall-1 チェックボックスを選択し、また Management Station チェックボックスを選択して下さい:
4. Cisco ルータの背後にある外部ネットワークのためのオブジェクトを ( 「inside\_cisco」と呼ばれる ) 設定するために Manage > Network objects > New > Network の順に選択して下さい。これは Cisco `access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255` コマンドの出典 ( 最初 ) ネットワークと一致するはずです。[Location] の [External] を選択します。
5. 外部 Cisco ルータ ゲートウェイのためのオブジェクトを Manage > Network objects > New > Workstation の順に選択して下さい ( 「cisco\_endpoint」と呼ばれる追加するために )。こ

これは暗号マップ名 コマンドが適用する Cisco インターフェイスです。[Location] の [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. これらのコマンドで一致するために DES 暗号化のための IKE プロパティを変更して下さい :`crypto isakmp policy #暗号化 DES`注: DES 暗号化はデフォルトです従って Cisco コンフィギュレーションで目に見えません。
8. これらのコマンドで一致するために SHA1 ハッシュに IKE プロパティを変更して下さい :`crypto isakmp policy #ハッシュ sha`注: SHA ハッシュアルゴリズムはデフォルトです従って Cisco コンフィギュレーションで目に見えません。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。これはこれらのコマンドで一致します:`crypto isakmp policy #authentication pre-share`
9. 事前共有キーを Cisco 暗号 `isakmp key` キー アドレスアドレス コマンドで一致するために設定するために『Edit Secrets』 をクリックして下さい:
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. これらのコマンドで一致するために IKE プロパティ DES 暗号化を変更して下さい:`crypto isakmp policy #暗号化 DES`注: DES 暗号化はデフォルトです従って Cisco コンフィギュレーションで目に見えません。
12. これらのコマンドで一致するために SHA1 ハッシュに IKE プロパティを変更して下さい :`crypto isakmp policy #ハッシュ sha`注: SHA ハッシュアルゴリズムはデフォルトです従って Cisco コンフィギュレーションで目に見えません。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。これはこれらのコマンドで一致します:`crypto isakmp policy #authentication pre-share`
13. 事前共有キーを暗号 `isakmp key` キー アドレスアドレス Cisco コマンドで一致するために設定するために『Edit Secrets』 をクリックして下さい。
14. [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. グリーン の Encrypt アイコンをクリックし、処理先頭に立の下で暗号化ポリシーを設定するために『Edit properties』 を選択して下さい。
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、`crypto ipsec transform-set rtpset esp-des esp-sha-hmac` コマンドの Cisco IPsec トランスフォームと一致するためにこれらの特性を変更して下さい :[Transform] の [Encryption + Data Integrity (ESP)] を選択します。暗号化アルゴリズムはデータ統合 SHA1 であるはずですが DES であり許可されたピアゲートウェイは外部ルータゲートウェイははずです ( 「 cisco\_endpoint 」 と呼ばれるである )。[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

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

[Output Interpreter Tool](#) ( OIT ) ( [登録ユーザ専用](#) ) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

- **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** — 電流 SA によって使用される設定を表示して下さい。

## 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役立つ情報について説明します。

### トラブルシューティングのためのコマンド

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。

- **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。

## 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。ルータが一致するために設定されない場合トンネルは失敗する可能性が高いです。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。

## チェックポイント

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。より多くの冗長なデバッグは下記のもので得ることができます:

```
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
```

注: 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。

Checkpoint の SA をクリアするこれらのコマンドを発行して下さい:

```
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」とプロンプトで発行します。

## デバッグの出力例

Configuration register is 0x2102

```
cisco_endpoint#debug crypto isakmp Crypto ISAKMP debugging is on cisco_endpoint#debug crypto
isakmp Crypto IPSEC debugging is on cisco_endpoint#debug crypto engine Crypto Engine debugging
is on cisco_endpoint# 20:54:06: IPSEC(sa_request): , (key eng. msg.) src= 172.18.124.35, dest=
172.18.124.157, src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy=
10.32.50.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur=
3600s and 4608000kb, spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1) 20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange 20:54:06: ISAKMP (0:1): sending packet to
172.18.124.157 (I) MM_NO_STATE 20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I)
MM_NO_STATE 20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0 20:54:06: ISAKMP
(0:1): found peer pre-shared key matching 172.18.124.157 20:54:06: ISAKMP (0:1): Checking ISAKMP
transform 1 against priority 1 policy 20:54:06: ISAKMP: encryption DES-CBC 20:54:06: ISAKMP:
hash SHA 20:54:06: ISAKMP: default group 1 20:54:06: ISAKMP: auth pre-share 20:54:06: ISAKMP
(0:1): atts are acceptable. Next payload is 0 20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0 20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP 20:54:06: ISAKMP (0:1):
received packet from 172.18.124.157 (I) MM_SA_SETUP 20:54:06: ISAKMP (0:1): processing KE
payload. message ID = 0 20:54:06: CryptoEngine0: generate alg parameter 20:54:06: ISAKMP (0:1):
processing NONCE payload. message ID = 0 20:54:06: ISAKMP (0:1): found peer pre-shared key
matching 172.18.124.157 20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1 20:54:06:
ISAKMP (0:1): SKEYID state generated 20:54:06: ISAKMP (1): ID payload next-payload : 8 type : 1
protocol : 17 port : 500 length : 8 20:54:06: ISAKMP (1): Total payload length: 12 20:54:06:
CryptoEngine0: generate hmac context for conn id 1 20:54:06: ISAKMP (0:1): sending packet to
172.18.124.157 (I) MM_KEY_EXCH 20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I)
MM_KEY_EXCH 20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0 20:54:06: ISAKMP
(0:1): processing HASH payload. message ID = 0 20:54:06: CryptoEngine0: generate hmac context
for conn id 1 20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157 20:54:06:
ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267 20:54:06: CryptoEngine0:
generate hmac context for conn id 1 20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I)
QM_IDLE 20:54:06: CryptoEngine0: clear dh number for conn id 1 20:54:06: ISAKMP (0:1): received
packet from 172.18.124.157 (I) QM_IDLE 20:54:06: CryptoEngine0: generate hmac context for conn
id 1 20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267 20:54:06: ISAKMP
(0:1): processing SA payload. message ID = 1855173267 20:54:06: ISAKMP (0:1): Checking IPsec
proposal 1 20:54:06: ISAKMP: transform 1, ESP_DES 20:54:06: ISAKMP: attributes in transform:
20:54:06: ISAKMP: encaps is 1 20:54:06: ISAKMP: SA life type in seconds 20:54:06: ISAKMP: SA
life duration (basic) of 3600 20:54:06: ISAKMP: SA life type in kilobytes 20:54:06: ISAKMP: SA
life duration (VPI) of 0x0 0x46 0x50 0x0 20:54:06: ISAKMP: authenticator is HMAC-SHA 20:54:06:
validate proposal 0 20:54:06: ISAKMP (0:1): atts are acceptable. 20:54:06:
IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.18.124.157, src=
172.18.124.35, dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4), src_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 20:54:06: validate proposal
request 0 20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267 20:54:06:
ISAKMP (0:1): processing ID payload. message ID = 1855173267 20:54:06: ISAKMP (0:1): processing
ID payload. message ID = 1855173267 20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ipsec allocate flow 0 20:54:06: ipsec allocate flow 0 20:54:06: ISAKMP (0:1): Creating
IPSec SAs 20:54:06: inbound SA from 172.18.124.157 to 172.18.124.35 (proxy 10.32.50.0 to
192.168.1.0) 20:54:06: has spi 0xA29984CA and conn_id 2000 and flags 4 20:54:06: lifetime of
3600 seconds 20:54:06: lifetime of 4608000 kilobytes 20:54:06: outbound SA from 172.18.124.35 to
172.18.124.157 (proxy 192.168.1.0 to 10.32.50.0) 20:54:06: has spi 404516441 and conn_id 2001
and flags 4 20:54:06: lifetime of 3600 seconds 20:54:06: lifetime of 4608000 kilobytes 20:54:06:
```

```
ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE 20:54:06: ISAKMP (0:1): deleting node
1855173267 error FALSE reason "" 20:54:06: IPSEC(key_engine): got a queue event... 20:54:06:
IPSEC(initialize_sas): , (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157, dest_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi=
0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4 20:54:06: IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157, src_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi=
0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4 20:54:06: IPSEC(create_sa): sa
created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi= 0xA29984CA(2727969994), sa_trans=
esp-des esp-sha-hmac , sa_conn_id= 2000 20:54:06: IPSEC(create_sa): sa created, (sa) sa_dest=
172.18.124.157, sa_prot= 50, sa_spi= 0x181C6E59(404516441), sa_trans= esp-des esp-sha-hmac ,
sa_conn_id= 2001 cisco_endpoint#sho cry ips sa interface: Ethernet0/0 Crypto map tag: rtp, local
addr. 172.18.124.35 local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0) remote
ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0) current_peer: 172.18.124.157 PERMIT,
flags={origin_is_acl,} #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14 #pkts decaps: 14,
#pkts decrypt: 14, #pkts verify 14 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0, #send errors 1, #recv errors
0 local crypto endpt.: 172.18.124.35, remote crypto endpt.: 172.18.124.157 path mtu 1500, media
mtu 1500 current outbound spi: 181C6E59 inbound esp sas: spi: 0xA29984CA(2727969994) transform:
esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto
map: rtp --More-- sa timing: remaining key lifetime (k/sec): (4607998/3447) IV size: 8 bytes
replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0x181C6E59(404516441) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2001, flow_id: 2, crypto map: rtp sa timing: remaining key lifetime (k/sec):
(4607997/3447) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:
cisco_endpoint#show crypto isakmp sa dst src state conn-id slot 172.18.124.157 172.18.124.35
QM_IDLE 1 0 cisco_endpoint#exit
```

## [関連情報](#)

- [IPSec ネゴシエーション/IKE プロトコル](#)
- [IPsec ネットワーク セキュリティの設定](#)
- [インターネット キー交換セキュリティ プロトコルの設定](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)