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

# 内容

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
トラブルシュート
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

# <u>概要</u>

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。これらのネットワークは、Cisco ルータ内部の 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

## <u>要件</u>

この設定例では、設定を開始する前に、ル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(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。

## <u>使用するコンポーネント</u>

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 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

(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。

### <u>表記法</u>

ドキュメント表記の詳細は、『<u>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。</u>

# <u>設定</u>

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、<u>Command Lookup</u> <u>Tool(登録</u>ユーザ専用)を使用してください。

## <u>ネットワーク図</u>

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。



### <u>設定</u>

このドキュメントでは次の設定を使用します。

- ・<u>ルータの設定</u>
- ・<u>チェックポイントファイアウォールの設定</u>

#### <u>ルータの設定</u>

#### Cisco 3600 ルータの設定

Current configuration : 1608 bytes

version 12.1

1

```
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
1
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
ip subnet-zero
no ip finger
1
ip audit notify log
ip audit po max-events 100
1
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1
authentication pre-share
crypto isakmp key ciscorules address 172.18.124.157
1
!--- 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
1
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
1
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
1
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
1
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
1
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
1
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

### <u>チェックポイントファイアウォールの設定</u>

チェックポイントファイアウォールを設定するには、次の手順を実行します。

 IKEライフタイムとIPsec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ライフタイムをシスコのデフォルトに一 致するように設定します。CiscoのデフォルトのIKEライフタイムは86400秒(=1440分)で あり、次のコマンドで変更できます。crypto isakmp policy #lifetime #設定可能なCisco IKEラ イフタイムは60 ~ 86400秒です。CiscoのデフォルトのIPsecライフタイムは3600秒で、 crypto ipsec security-association lifetime seconds #コマンドで変更できます。設定可能な Cisco IPsecライフタイムは120 ~ 86400秒です。

Properties Setup					
High Availability   IP Pool NAT   Acces Security Policy   Traffic Control   Services   L Authentication   SYNDefender   LDAP	ss Lists Desktop Security Log and Alert Security Servers Encryption ConnectControl				
SKIP Enable E <u>x</u> portable SKIP Change SKIP Session Key :	Manual IPSEC SPI allocation range (hex):				
Every     120     Seconds (0 for infinity)       or     Every     10485760       Bytes (0 for infinity)	Erom 100 To ffff				
IKE     Renegotiate I <u>K</u> E Security Associations every     Renegotiate IPSEC Security Associations every	1440 minutes 3600 seconds				
- WordPad Command Prompt Transformed Prompt					

 Manage > Network objects > New (またはEdit) > Networkの順に選択し、Checkpointの背後にある内部ネットワーク(cpinside)のオブジェクトを設定します。これは、Cisco accesslist 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(2番目)ネットワークと一致する必要があります。[Location]の[Internal]を選択します。

Network Properties
General NAT
Name: cpinside
IP Address: 10.32.50.0 Get address
Net <u>M</u> ask: 255.255.255.0
Comment: Color:
Location: ● Internal ● External ● Allowed ● Disallowed
OK Cancel Help

3. Manage > Network objects > Editの順に選択して、set peer 172.18.124.157コマンドで Ciscoルータが指すRTPCPVPN Checkpoint(ゲートウェイ)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 で Gateway を選択します。 [Modules Installed]で、[VPN-1 & FireWall-1]チェックボックスを選択し、[Management Station]チェックボックスを選択します。

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
Name: RTPCPVPN
IP Address: 172.18.124.157 Get address
Comment: Firewalled gateway to internet
Location:     Type:       Internal     External
Modules Installed
✓ VPN-1 & FireWall-1 Version: 4.1
☐ FloodGate-1 Version: 4.1 ▼
Compression Version: 4.1
Management Station Color:
OK Cancel Help

[Manage] > [Network objects] > [New] > [Network]を選択して、Ciscoルータの背後にある外部ネットワーク(「inside\_cisco」と呼ばれる)のオブジェクトを設定します。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コマンドの送信元(最初)ネットワークと一致する必要があります。[Location]の[External]を選択します。

Network Properties
General NAT
<u>Name:</u> inside_cisco
IP Address: 192.168.1.0
Net <u>M</u> ask: 255.255.255.0
Comment: Cojor:
Location: ○ Internal ● External ● Broadcast: ● Allowed ● Disallowed
OK Cancel Help

5. 外部のCiscoルータ**ゲートウェイにオブジェクトを追加するには、[管理] > [ネットワークオ ブジェクト] > [新規作成] > [ワークステーション]を選択します(「cisco\_endpoint」と呼ば れる)。 これは、crypto map nameコマンドが適用される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。** 

Workstation Properties	×			
General Interfaces SNMP NAT VPN				
<u>N</u> ame: <u>cisco_endpoint</u>				
IP Address: 172.18.124.35 Get address				
<u>C</u> omment:				
Location:Type: ○ Internal ⊙ External ○ Host ⊙ Gateway				
Modules Installed				
□ VPN-1 & <u>F</u> ireWall-1 Version: 4.1 <u>Get</u> <u>Get</u>				
FloodGate-1 Version: 4.1				
Compression Version: 4.1				
■ Management Station Color: ▼				
OK Cancel Help				

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。

Workstation Properties	×			
General Interfaces SNMP NAT	Certificates VPN Authe			
Domain:       Encryption schemes defined:         ① Disabled       ✓ Manual IPSEC         ② Dther:       ✓ Manual IPSEC         ② Dinside       ✓ Manual IPSEC         ③ Dinside       ✓ Manual IPSEC         ⑤ Dinside       ✓ Manual IPSEC         ⑤ Dinside       ✓ Manual IPSEC         ⑥ Dinside       ✓ Manual IPSEC         ⑥ Dinside       ✓ Manual IPSEC         ○ Dinside       ✓ Manual IPSEC         ○ Dinside       ✓ Manual IPSEC				
Traffic Control Logging				
OK Ca	ncel Help			

- 7. DES暗号化のIKEプロパティを次のコマンドと一致するように変更します。crypto isakmp policy #encryption des注: DES暗号化がデフォルトであるため、Ciscoの設定では表示され ません。
- 8. 次のコマンドに一致するように、IKEプロパティをSHA1ハッシュに変更します。crypto isakmp policy #hash sha注: SHAハッシング</mark>アルゴリズムはデフォルトであるため、シスコ の設定では表示されません。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、次のコマンドと一致します。crypto isakmp policy #authentication pre-

General Interfaces SNMP NAT Certificates	VPN Authe				
KE Properties	Þ				
General					
Key <u>N</u> egotiation Encryption Method(s):	- <u>H</u> ash Method: -				
□ 🖾 CAST					
JL ⊨≊ 3DES					
Authentication Method:					
✓ Pre-Shared Secret Edit Secrets					
Public Key Signatures     Configure					
Supports Approxition Model - M. Supports					
	soublets				
OK Cancel H					

9. [Edit Secrets]をクリックして、事前共有キーをCisco crypto isakmp key key addressコマン ドと一致させるように設定します。

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
IKE Properties
General
Shared Secret
Shared Secrets List:
Peer Name       Shared Secret         Cisco_endpoint       ****         Edit         Remove
OK Cancel
OK Cancel Help
OK Cancel Help

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。

Workstation Properties	×			
General Interfaces SNMP NAT				
Domain:	Encryption schemes defined:			
C <u>D</u> isabled	Manual IPSEC			
© ⊻alid Addresses(of Interfaces)				
	🗆 📷 SKIP			
🚆 inside_cisco 🔻				
Exportable for SecuFlemote	<u>E</u> dit			
Traffic Control Logging      Ium on Traffic Control Logging				
OK Car	ncel Help			

- 11. 次のコマンドに一致するように、IKEプロパティDES暗号化を変更します。crypto isakmp policy #encryption des注:DES暗号化がデフォルトであるため、Ciscoの設定では表示され ません。
- 12. 次のコマンドに一致するように、IKEプロパティをSHA1ハッシュに変更します。crypto isakmp policy #hash sha注: SHAハッシング</mark>アルゴリズムはデフォルトであるため、シス コの設定では表示されません。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、次のコマンドと一致します。crypto isakmp policy #authentication

General Interfaces SNMP NAT Certificates VPN Authe	•				
KE Properties	×				
General					
Key <u>N</u> egotiation Encryption Method(s): <u>Hash Method</u> : MD5					
□ ➢ CAST □ ➢ 3DES ☑ SHA <u>1</u>					
Authentication Method:					
Image: Pre-Shared Secret       Edit Secrets         Image: Public Key Signatures       Configure					
Supports Aggresive Mode 🔽 Supports Subnets					
OK Cancel Help					
e-share					

13. Edit Secretsをクリックして、事前共有キーをcrypto isakmp key key address address *Ciscoコマンドと一致さ*せるように設定します。

IKE Properties
General
Shared Secret 🔀
- Shared Secrets List:
Peer Name Shared Secret
RTPCFVPN **** <u>E</u> dit
Bernova
OK Cancel
OK Cancel Help

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。

Ĩ	RTP	CPVPN - Check P	oint Policy Editor				_ 🗆 🗵
ŀ	ile <u>E</u> d	it <u>V</u> iew <u>M</u> anage	Policy <u>W</u> indow <u>H</u>	elp			
	- 5	🖪 🔍 👗 🖻	◎ 월 종 办	B.   🕫 🙋	🖆 📙 🖀 🐣	" 🖦 🖳 🦡 🕪	🛃 🐻 🎹 🚯
	Sec	urity Policy - Standard	l 🛅 Address Trans	slation - Standard	😿 Bandwidth Po	licy - Standard	
	No.	Source	Destination	Service	Actio	n Track	< In <mark></mark> ≜
Ì	1	💂 inside_cisco	💂 cpinside	Any	Encry	pt 🚺 Long	
ļI.	•						•
F	or Help,	press F1		R	TPCPVPN	Read/Write	

15. 緑色の[暗号化]アイ**コンをクリ**ックし、[プロ**パティの編**集]を選択して、[操作]見出しの下に 暗号化ポリシーを構成します。

arity Policy - Standard 🛛 📇 Address Translation - Standard 🛛 😿 Bandwidth Policy - Standard						
∼ FVV1 Host	∼ Ldap-Servers	😰 Idap	accept			
∼ FVV1 Host	∼ Logical-Servers	∼ load_agent	accept			
😓 inside_cisco	cpinside	Any	dit properties	hg .		
		icmp dest-unreach	Edit Encryption			
		icmp echo-request	accept	am 🦵		
		icmp info-reply	drop			
Any	Any	icmp mask-reply	🚺 😑 reject			
-				•		

16. IKE を選択してから Edit をクリックします。

Encryption Properties	×
General	
Encryption schemes defined:	
Edit	
OK Cancel Help	

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ように、次のプロパティを変更します。 [Transform] の [Encryption + Data Integrity (ESP)] を選択します。 暗号化アルゴリズムは DES、データ整合性はSHA1、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(「 cisco\_endpoint」と呼ばれる) である必要があります。 [OK] をクリックします。

IKE Properties	×
General	
☐ransform: ⓒ Encryption + Data Integrity (ESP)	
O Data Integrity Only (AH)	
Encryption Algorithm: DES	
Data Integrity SHA1	
Allowed Peer Gateway:	
Use Perfect Forward Secrecy	
OK Cancel Help	

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。

# <u>確認</u>

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。

<u>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</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。

- **show crypto isakmp sa**:ピアにおける現在のIKE Security Association (SA;セキュリティア ソシエーション)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。

# <u>トラブルシュート</u>

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。

# <u>トラブルシューティングのためのコマンド</u>

- 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。

#### <u>ネットワーク集約</u>

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。ルータが一致するように設定されていない場合、トンネルは失敗する可能性があり 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。

### <u>チェックポイント</u>

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 注:これはMicrosoft Windows NTのインストールです。

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。

## <u>デバッグの出力例</u>

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
                   : 500
       port
       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
                    SA life duration (VPI) of 0x0 0x46 0x50 0x0
20:54:06: ISAKMP:
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
                 lifetime of 3600 seconds
20:54:06:
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

 $\texttt{cisco\_endpoint} \texttt{\texttt{#exit}}$ 



- 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
- ・Internet Key Exchange 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