# 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 <u>前提条件</u> 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 トラブルシュート Cisco ルータ 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。

- ・ルータ内部のプライベート ネットワーク 172.16.15.x
- Checkpoint<sup>TM Next Generation (NG)内のプライベート ネットワーク 192.168.10.x</sup>

## <u>前提条件</u>

### <u>要件</u>

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。

## <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 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)
- ・CheckpointTM 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>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>表記法</u>

ドキュメントの表記法の詳細は、「<u>シスコ テクニカル ティップスの表記法</u>」を参照してください 。

## <u>Cisco 1751 VPN ルータの設定</u>

Cisco VPN 1751 ルータ
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname sv1-6
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
<pre>! Internet Key Exchange (IKE) configuration. crypto</pre>
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
1
crypto map aptmap 1 ipsec-isakmp
 set peer 209.165.202.129
 set transform-set aptset
 match address 110
!
interface Ethernet0/0
 ip address 209.165.202.226 255.255.254
 ip nat outside
 half-duplex
 crypto map aptmap
1
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
```

## <u>Checkpoint NG の設定</u>

The CheckpointTM 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、 CheckpointTM NG Policy Editor を使用してこのポリシーをインストールすると、CheckpointTM 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、CheckpointTM 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     O Not included	
OK Cancel Help	

Network Properties - Cisco_Network	×
General NAT	
Name: Cisco_Network	
IP Address: 172.16.15.0	
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。 Checkpoint<sup>TM 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 <sup>ます。</sup>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。</sup>

Workstation Properties -	chef 🔀
General Topology NAT VPN Authentication Management ⊕ Advanced	General   Name:   Chef   IP Address:   209.165.202.129   Get address   Comment: CP_Server Color:    Color:   Color:   Type:   Host   Gateway   Check Point Products   Check Point products installed:   VPN-1 & FireWall-1   FloodGate-1   Policy Server   Primary Management Station
	Object Management         Image: Managed by this Management Server (Internal)         Image: Managed by another Management Server (External)         Secure Internal Communication         Image: Communication         Image: DN:         Image: Communication Properable VPN Device         Image: OK         Image: OK         Image: OK         Image: OK         Image: OK         Image: OK

Workstation Properties - (	Cisco_Router	×
General	General	
Topology NAT	Name: Cisco_Router	
	IP Address: 209.165.202.226 Get address	
	Comment: Cisco_VPN_Router	
	Color:	
	Type: C Host 💽 Gateway	
	Check Point Products	
	Check Point products installed: Version NG Cet Version	
	VPN-1 & FireWall-1 FloodGate-1 Policy Server Secondary Management Station	
	Object Management	
	C Managed by this Management Server (Internal)	
	C Managed by another Management Server (External)	
	✓ Interoperable VPN Device	
	OKCancelHe	p die

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

Workstation Properties -	chef	×
General Topology NAT VPN Authentication Management T Advanced	VPN     Encryption schemes     Image: Imag	
	Nickname DN Certificate Authority	
	Add Edit Remove	
	OK Cancel Help	

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

IKE Properties	×
General	
Support key exchange encryption w	ith: Support data integrity with:
Support authentication methods:	
✓ Pre-Shared Secret	Edit Secrets
Public Key Signatures	Specify
VPN-1 & FireWall-1 authenticat	ion for SecuRemote (Hybrid Mode)
<u>-</u>	
	Advanced
OK Car	ncel Help

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。

Shar	red Secret		×
Г	Shared Secrets List: -		
	Peer Name	Shared Secret	
	chet		Edit
			Remove
	Enter secret: aptrul	es Set	
	ОК	Cancel	Help

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。

M Sec	unity - APTPolicy 🗮 /	Address Translation - AP	TPolicy 📴 Deskto	op Security - St	andard				
NO.	SOURCE	DESTINATION	SERVICE	ACT	TION	TRACK	INSTALL ON		
1	부 CP_Network 부 Cisco_Network	부 CP_Network 부 Cisco_Network	* Any	S Encry	pt Edit or o	E Log	Gateways	*	An
2	🖈 Any	* Any	* Any	🔘 drop	Add End Edit End	ryation	Gateways	*	An
• Nam	8	IP	Comment		accept     drop     cept     cept     cept				•
🕌 chei 🔲 Cisc	: o_Router	209.165.1 209.165.1	02.129 CP_Serve 02.226 Cisco_VP	er N_Router	Client Client	Auth In Auth In Forypt			
					Query C Clear Q	Column			4

7. <u>[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。</u>

Encryption Properties	×
General	
Encryption schemes defined:	
E dit	
OK Cancel Help	

8. IKE の設定を確認します。

IKE Properties		×
General		
Transform		[
Encryption + Data Integrity	(ESP)	
O Data Integrity Only (AH)		
Encryption Algorithm:	3DES	•
Data Integrity	MD5	•
Compression method:	None	•
Allowed Peer Gateway:	Cisco_Router	•
Use Perfect Forward Secrecy		
Use DH Group:	Group 1 (768 bit)	
Perform IP Pool NAT		
OK Ca	ncel Help	

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。

Advanced IKE properties				×
Use UDP encapsulation				
	UDP VP	N1_IPSEC_	encapsi 💌	
Support Diffie-Hellman groups				
	Group	o 1 (768 bit) - D (1904 bit		
	Group	o 2 (1024 bi o 5 (1536 bi	a t)	
Deliverine Decementary	<u> </u>	•		
Rekeying Parameters				
Renegotiate IKE security associa	itions	30	)	Minutes
Renegotiate IPSEC Security asso	ociations e	every 36	i00 🛨	Seconds
🔲 Renegotiate IPSEC Security -	associatio	ns every 50	0000	KBytes
Miso				
Support IP compression for S	ecureClier	nt		
Support aggresive mode				
Support key exchange for sul	bnets			
ОК С	ancel		Help	

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。

The chef - Check Point Policy Editor - APTPolicy						
File Edit View Manage Rules	Policy Topology Search Window	Help				
🖬 ☜   🐰 🖸 🛍    🏪	Verify Install	° == "≡ =×   ♥ ≛ ∰   \?				
<b>°ta 🔲   8::: }*</b>   2↓ 8↓	Uninstall					
┺॑(� @ ┋ や ⊙	Access Lists	Address Translation - APTPolicy				
E-T+ Network Objects	Install Users Database	DESTINATION	CEDVICE			
Workstation	Management High Availability	DESTINATION	JENVICE			
Cisco_Router	Global Properties	・				
Network     Sisco_Network	2 * Any	* Any	🗙 Any			

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。

Install Policy	×
APTPolicy.W: Security Policy Script generated into APTPolicy.pf APTPolicy: Compiled OK.	
	₹ ₹

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。

Install Policy	×
APTPolicy.W: Security Policy Script generated into APTPolicy.pf APTPolicy: Compiled OK.	<u> </u>
Installing VPN-1/FireWall-1 policy On: chef	
VPN-1/FireWall-1 policy installed successfully on chef	
VPN-1/FireWall-1 policy installation complete	
Close	

## <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>Cisco ルータの検証</u>

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。

#### <u>Checkpoint NG の検証</u>

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

1	hef - Check I	Point Log Vi	ewer - [fw.log]								
Fle	Mode Edit	Selection \	Vew Tools Window H	elp							
65	🗳 🖬 🛛	og	- = A 🕈 🛓	💕 🗐	<b>B</b> 👼		🖩 🇞 🟭 '	la 🔊   🐔			
No.	Date	Time	Product	inter.	Origin	Турс	Action	Service	Source	Destination	Proto.
4	18Jul2002	12.41:12	VPN-1 8 FireWall-1	📑 dae .	. chet	🔳 log	0- key instal		chef	Cisco_Router	
5	18Jul2002	12:41:13	VPN-1 & FireWall-1	💽 dae	. chet	🔳 log	0- key instal		chef	Gisco_Router	
6	18Jul2002	12:41:13	VPN-1 8 FireWall-1	EL9	. chef	log	📷 encrypt	teinet	GARRISON	Cisco_Router	top

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。

Chef - Check Point System Statu	is Window Help		LOX				
2 ■ A II A # A # A # O # A							
Modules	IP Address	VPN-1 Details					
B M chef		Status:	0K				
e- Chef	209.165.202.12	Packets					
FireWal-1		Encrypted:	38				
* Management		Decrypted:	37				
SVN Foundation		Errors					
		Encryption errors:	0				
		Decryption errors:	0				
		IKE events errors:	0				
		Hardware					
		HW Vendor Name:	none				
		HW Status:	none				

## <u>トラブルシュート</u>

<u>Cisco ルータ</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。

このほかのトラブルシューティングについては、「<u>IP Security のトラブルシューティング</u>-<u>debug コマンドの理解と使用</u>」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<u>の重要な情報』を参照してください</u>。

・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。

18:05:32: ISAKMP (0:0): received packet from

- ・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

```
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 = 018:05:33: ISAKMP (0:1): processing HASH payload. message ID = 018:05:33: 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 = -133537110318:05:33: ISAKMP (0:1): processing SA payload. message ID = -133537110318:05:33: 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 = -133537110318:05:33: ISAKMP (0:1): processing ID payload. message ID = -133537110318:05:33: ISAKMP (0:1): processing ID payload. message ID = -133537110318:05:33: 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

```
18:05:33: ISAKMP (0:1): Node -1335371103,
   Input = IKE_MESG_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_MESG_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
```

209.165.202.129 (R) QM\_IDLE

#### sv1-6#show crypto isakmp sa

dst src state conn-id slot 209.165.202.226 209.165.202.129 QM\_IDLE 1 0

```
sv1-6#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:
```

#### sv1-6#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



- IPSec に関するサポート ページ
- ・<u>テクニカルサポート Cisco Systems</u>