체크포인트 NG와 라우터 간 IPSec 터널 구성

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>네트워크 다이어그램</u> <u>표기 규칙</u> <u>Cisco 1751 VPN 라우터 구성</u> <u>체크포인트 NG 구성</u> <u>다음을 확인합니다.</u> <u>Cisco 라우터 확인</u> 체<u>크포인트 NG 확인</u> <u>문제 해결</u> <u>Cisco 라우터</u> <u>관련 정보</u>

<u>소개</u>

이 문서에서는 사전 공유 키를 사용하여 IPSec 터널을 형성하여 두 개의 프라이빗 네트워크에 연결 하는 방법을 설명합니다.

- 라우터 내의 172.16.15.x 프라이빗 네트워크.
- CheckpointTM NG(Next Generation) 내부 192.168.10.x 프라이빗 네트워크

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 문서에 설명된 절차는 이러한 가정을 기반으로 합니다.

- Checkpoint[™] NG 기본 정책이 설정되었습니다.
- 모든 액세스, NAT(Network Address Translation) 및 라우팅 설정이 구성됩니다.
- 라우터 내부 및 CheckpointTM NG 내부에서 인터넷 플로우로 이동하는 트래픽.

<u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

Cisco 1751 Router

- Cisco IOS® 소프트웨어(C1700-K9O3SY7-M), 버전 12.2(8)T4, 릴리스 소프트웨어(fc1)
- ^{CheckpointTM} NG 빌드 50027

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



<u>표기 규칙</u>

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

<u>Cisco 1751 VPN 라우터 구성</u>

Cisco VPN 1751 Router
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
<pre>! IPSec configuration. crypto isakmp key aptrules</pre>
address 209.165.202.129
1

```
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 209.165.202.226 255.255.255.224
 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
```

<u>체크포인트 NG 구성</u>

CheckpointTM NG는 객체 지향 컨피그레이션입니다. 네트워크 객체 및 규칙은 설정할 VPN 컨피그 레이션과 관련된 정책을 구성하기 위해 정의됩니다. 그런 다음 CheckpointTM NG 정책 편집기^를 사 용하여 VPN 컨피그레이션의 ^{CheckpointTM} NG 측^을 완료합니다.

1. Cisco 네트워크 서브넷 및 ^{CheckpointTM} NG 네트워크 서브넷을 네트워크 개체로 생성합니다. 이것이 암호화된 것입니다. 객체를 생성하려면 **Manage(관리) > Network Objects(네트워크 객 체)를** 선택한 다음 New(새로 만들기) **> Network(네트워크)를 선택합니다**. 적절한 네트워크 정 보를 입력한 다음 **확인**을 클릭합니다.다음 예에서는 CP_Network 및 Cisco_Network라는 객체 집합을 보여 줍니다

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: 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 O Not included
OK Cancel Help

2. Cisco_Router 및 Checkpoint_NG 객체를 워크스테이션 객체로 생성합니다. 이는 VPN 디바이 스입니다. 객체를 생성하려면 **관리 > 네트워크 객체**를 선택한 다음 새로 만들기 **> 워크스테이** *션*을 **선택합니다**.초기 CheckpointTM NG 설정 중에 생성된 ^{CheckpointTM} NG 워크스테이션 객 체^를 사용할 수 있습니다. 워크스테이션을 **게이트웨이** 및 상호 운용 가능한 **VPN 장치**로 설정 하는 옵션을 **선택합니다**.다음 예에서는 chef 및 Cisco_Router라는 객체 집합을 보여 줍니다

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	x
General	General	
Topology NAT	Name:	Cisco_Router
VPN Advanced	IP Address:	209.165.202.226 Get address
	Comment:	Cisco_VPN_Router
	Color:	
	Туре:	C Host 🖲 Gateway
	Check Point P	Products
	Check Po	int products installed: Version NG Get Version
	□VPN-1 & F □FloodGate	FireWall-1
	Policy Ser	ver y Management Station
	Object Manag	gement
	C Managed	by this Management Server (Internal)
	C Managed	by another Management Server (External)
	✓ Interoper	rable VPN Device
		OK Cancel Help

3. VPN 탭에서 IKE를 구성한 다음 Edit(수정)를 클릭합니다

.

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

4. 키 교환 정책을 구성하고 Edit Secrets를 클릭합니다

IKE Properties	
General	
Support key exchange encryption with:	
Support authentication methods:	
Pre-Shared Secret Edit Secrets	
Public Key Signatures Specify	
VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)	
Advanced	
OK Cancel Help	
5. 미리 공유한 키를 사용하도록 설정한 다음 구성 창이 사라질 때까지 OK(혹	* 안)를 여러 번 클릭 x
Shared Secrets List:	
Peer Name Shared Secret	
Edit	
Remove	
Enter secret: aptrulesSet	
한니다 OK Cancel Help	
합니다	

6. Rules > Add Rules > Top을 선택하여 정책에 대한 암호화 규칙을 구성합니다.상단의 규칙은 암호화를 우회할 수 있는 다른 규칙보다 먼저 수행되는 첫 번째 규칙입니다. 여기에 표시된 대 로 CP_Network 및 Cisco_Network를 포함하도록 Source 및 Destination을 구성합니다. 규칙의 Encrypt Action(암호화 작업) 섹션을 추가한 후 Action(작업)을 마우스 오른쪽 버튼으로 클릭하 고 Edit Properties(속성 편집)를 선택합니다

M Sec	unity - APTPolicy 🗮 /	Address Translation - AP	TPolicy 📴 Deskto	op Security - St	andard			
NO.	SOURCE	DESTINATION	SERVICE	ACT	ION	TRACK	INSTALL ON	
1	부 CP_Network 부 Cisco_Network	부 CP_Network 부 Cisco_Network	★ Any	Encry	pt Edit oro	E Log	Gateways	* An
2	* Any	* Any	* Any	i drop	Add End Edit End	ryption	Gateways	🗙 An
• Nan	10	10	Comment		 accept drop reject 	•		Þ
📔 che 🔲 Ciso	f io_Router	209.165.7 209.165.7	02.129 CP_Servi 02.226 Cisco_VP	er N_Router	Clent / Clent / Session Encryp Clent /	Auth Auth on Auth Encrypt		
					Query C Clear Q	Column		

7. IKE를 선택하고 강조 표시한 상태에서 Edit(**수정)**를 클릭합니다

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

8. IKE 컨피그레이션을 확인합니다

IKE Properties	x
General	
Transform	
Encryption + Data Integrit	y (ESP)
C 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	ancel Help

9. Cisco 디바이스와 다른 IPSec 디바이스 간에 VPN을 실행하는 경우의 주요 문제 중 하나는 키 교환 재협상입니다. Cisco 라우터의 IKE 교환에 대한 설정이 CheckpointTM NG에 구성된 설 정과 정확히 ^{동일한지} 확인합니다.**참고:** 이 매개변수의 실제 값은 특정 회사 보안 정책에 따라 달라집니다.이 예에서 <u>라우터의 IKE 컨피그레이션은</u> lifetime 1800 명령을 사용하여 30분으로 설정되었습니다. CheckpointTM NG에서 동일한 값을 ^{설정해야} 합니다.CheckpointTM ^{NG}에서 이 값을 설정하려면 Manage Network Object(네트워크 개체 관리)를 선택한 다음 ^{CheckpointTM} NG 개체를 선택하고 Edit(수정)를 클릭합니다. 그런 다음 VPN을 선택하고 IKE를 수정합니다. Advance를 선택하고 Rekeying Parameters를 구성합니다. CheckpointTM ^{NG} 네트워크 개체 에 대한 키 교환을 구성한 후 Cisco_Router 네트워크 개체에 대해 키 교환 재협상에 대해 동일 한 컨피그레이션을 수행합니다.**참고:** 라우터에 구성된 그룹과 일치하도록 올바른 Diffie-Hellman 그룹이 선택되었는지 확인합니다

Advanced IKE properties				×
Use UDP encapsulation				
	UDP VPN1	_IPSEC_encaps	. 🔻	
Support Diffie-Hellman groups ———				
	Group 1	(768 bit)		
	Group 2	: (1024 bit) i (1536 bit)		
		(1000 DK)		
Rekeying Parameters				
Renegotiate IKE security associa	tions	30	•	Minutes
Renegotiate IPSEC Security asso	ciations eve	ary 3600	÷	Seconds
Renegotiate IPSEC Security a	associations	every 50000	- A-	KBytes
Misc				
Support IP compression for S	ecureClient			
Support aggresive mode				
Support key exchange for sub-	onets			
	,			
OK C	ancel	Help		

10. 정책 구성이 완료되었습니다. 정책을 저장하고 Policy(정책) > Install(설치)을 선택하여 활성 화합니다

File Edit View Manage Rules	Policy Topology Search Window	Help		
🖬 � ‰ 🖬 🏪	Verify Install	°ݠ▯∝│♥	🛔 🛃 🗍 🕅	
°t: [? Ź↓ @↓	Uninstall			
<u>₽ q q @ 5 2 0</u>	Access Lists	Address Translation - APTPolicy 🛙 🛅 Deskt		
E	Install Users Database	DESTINATION	CEDVICE	
Workstation	Management High Availability	DESTINATION	JENVICE	
Cisco_Router	Global Properties	부 Cisco_Network 부 CP_Network	🗙 Any	
	2 * Any	* Any	* Any	

정책이 컴파일될 때 설치 창에 진행 정보가 표시됩니다

Install Policy		×
APTPolicy.W: Security Policy S APTPolicy: Compiled OK.	icript generated into APTPolicy.pf	
-		V
	Abort	

창에 정책 설치가 완료되었음을 알리는 메시지가 나타나면 **Close(닫기**)를 클릭하여 절차를 완료합니다

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	
	T
Close	

<u>다음을 확인합니다.</u>

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

<u>Cisco 라우터 확인</u>

일부 show 명령은 <u>출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면</u> show 명 령 출력의 분석 결과를 볼 수 있습니다.

• show crypto isakmp sa - 피어의 현재 IKE SA(Security Association)를 모두 표시합니다.

• show crypto ipsec sa - 현재 SA에서 사용하는 설정을 표시합니다.

<u>체크포인트 NG 확인</u>

로그를 보려면 Window > Log Viewer를 선택합니다.

1 20	hef - Check I	Point Log Vi	ewer - [fwJog]								
Fle	Mode Edit	Selection \	View Tools Window He	slp							
69 🖆 🖬 Log 🔹 🗛 🕈 🛓 🗳 🖩 🖬 😸 🗐 🚟 🖬 🇞 🏭 😘 🕗 🔋											
No.	Date	Time	Product	Inter.	Origin	Турс	Action	Service	Source	Destination	Proto.
4	18Jul2002	12.41:12	VPN-1 & FireWall-1	📑 dse	. chet	🔳 log	0- key instal		chef	Cisco_Router	
5	18Jul2002	12.41:13	VPN-1 8 FireWall-1	💽 dae	. chet	🔳 log	0- key instal		chef	Cisco_Router	
6	18Jul2002	12:41:13	VPN-1 & FireWall-1	EL9	. chef	🔳 log	📷 encrypt	teinet	GARRISON	Cisco_Router	top

시스템 상태를 보려면 창 > 시스템 상태를 선택합니다.

📅 chef - Check Point System Statu	\$							
File View Modules Products Tools	Window Help							
Modules	IP Address	VPN-1 Details						
🖃 📝 chef		Status:	OK .					
E- III chef	209.165.202.12	Packets						
		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					
1								

문제 해결

<u>Cisco 라우터</u>

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

추가 문제 해결 정보는 IP 보안 문제 해결 - 디버그 명령 이해 및 사용을 참조하십시오.

참고: debug 명령을 실행하기 전에 <u>디버그 명령에 대한 중요 정보를 참조하십시오</u>.

- debug crypto engine 암호화 및 해독을 수행하는 암호화 엔진에 대한 디버그 메시지를 표시합니다.
- debug crypto isakmp IKE 이벤트에 대한 메시지를 표시합니다.
- debug crypto ipsec IPSec 이벤트를 표시합니다.
- clear crypto isakmp 모든 활성 IKE 연결을 지웁니다.

• clear crypto sa - 모든 IPSec SA를 지웁니다. 디버그 로그 출력 성공

```
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) OM 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_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
```

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): (172.16.15.0/255.255.0/0/0) 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:

${\tt sv1-6}\#{\tt show}$ 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

<u>관련 정보</u>

- IPSec 지원 페이지
- Technical Support Cisco Systems