ASA에서 ASDM 또는 CLI를 사용하여 IKEv1 IPsec Site-to-Site 터널 구성

목차

<u>소</u>개 사전 요구 사항 요구 사항 사용되는 구성 요소 구성 네트워크 다이어그램 ASDM VPN 마법사를 통해 구성 CLI를 통해 구성 ASA 버전 8.4 이상에 대해 사이트 B 구성 ASA 버전 8.2 이하에 대한 사이트 A 구성 그룹 정책 다음을 확인합니다. ASDM CLI 1단계 2단계 문제 해결 ASA 버전 8.4 이상 ASA 버전 8.3 이전

소개

이 문서에서는 소프트웨어 버전 9.2.x를 실행하는 Cisco 5515-X Series ASA(Adaptive Security Appliance)와 소프트웨어 버전 8.2.x를 실행하는 Cisco 5510 Series ASA 간에 IKEv1(Internet Key Exchange version 1) IPsec 사이트 대 사이트 터널을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 엔드 투 엔드 IP 연결이 설정되어야 합니다.
- 다음 프로토콜을 허용해야 합니다. IPsec 컨트롤 플레인의 UDP(User Datagram Protocol) 500 및 4500IPsec 데이터 플레인용 ESP(Encapsulating Security Payload) IP Protocol 50

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.2를 실행하는 Cisco 5510 Series ASA
- 소프트웨어 버전 9.2를 실행하는 Cisco 5515-X ASA

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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 ASDM(Adaptive Security Device Manager) VPN 마법사 또는 CLI를 통해 사이트 대 사이트 VPN 터널을 구성하는 방법에 대해 설명합니다.

네트워크 다이어그램

이 토폴로지는 이 문서 전반의 예에 사용됩니다.



ASDM VPN 마법사를 통해 구성

ASDM 마법사를 통해 사이트 대 사이트 VPN 터널을 설정하려면 다음 단계를 완료하십시오.

1. ASDM을 열고 Wizards > VPN Wizards > Site-to-site VPN Wizard.

oli Words Window Help					
Satury Ward.				type type to search	i alta
					CIS
VDN Miserds * Sterio site VTN Waard.					
Ber High Arailability and Scalability Waard. And Second STM Ellipside					
Unified Conversariation Wood Cherdles 32, VPN Waard					
ASDM Selectity Cardinate Waard. IPsec (REv1) Remote Access VPU Manet.	Enterface Status				
Pashat Capture Weard.	Interface.	IP Aldress Not	Une	108	show
	ACON	10 105 100 100/24	0	0.4	
Herritane distante	inette	93.2.2.2.24	0.0	0.0	0
AGA Version: SLEDDP Device upone: Std /5 44m 05	inside 2	10.4.4.1/24	0.0	0.0	
ADDITED AND DEVELOPMENT ADDITION ADDITIONA ADDITION ADDITIONA ADDITICO ADDITICO ADDITICO ADDITICO ADDITICO ADDITICO ADDITICO ADDITICO ADDIT	outside	172.16.1.1/24	0.0	0.0	1
Tarrai Picele Self and Construction Self and					
	Select an interface 1	to view input and output Rbpo			
WIT Desires	Falson Dake				
Disect @ Disrobus S3, White AnyConnect Clerit: @ Databas	Fallorer not config.	ured: Click the link to configure it.			Sand
System Resources Status	TearRestown				
(Pultage (server)	Connections Per S	iecond Licage			
	-	0.27	11.00	<u> </u>	
(8404 1034 1037 6030 6030 6040	U0P 0	TOP: 0 Total 6		1000	1.2.2
Henory Litage (HB)	In this Drawface	A state from the Territory March			
	1	CONTRACTOR AND A CONTRACTOR OF A CONTRACTOR AND A CONTRAC			
+530					
4048 000					
500					
1840-8 10.38 10.37 10.38 10.30 10.40	10.98	10.27	43 OE	40.00	40-40
Details.	Povt Spin	1 OvbutResi 0			
Latert ASIIN Systep Resource					10 8
ASS/M kogging is disabled. To enable AS	P boging with informational lan Gnable Logging	vel, dick the button below.			
nd successful de		000	is 1	100	A word prove

2. 클릭 Next 마법사 홈 페이지가 나타납니다.

VPN Wizard	Introduction
Land Land Land Land Land Land Land Land	Use this ward to setup new site-to-site VPN tunnel. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol.
	Here is a <u>video</u> on how to setup a site-to-site VPN connection.
	< Bady Next > Cance Help

참고: 최신 ASDM 버전에서는 이 컨피그레이션을 설명하는 비디오에 대한 링크를 제공합니다. 3. 피어 IP 주소를 구성합니다. 이 예에서는 사이트 B에서 피어 IP 주소가 192.168.1.1로 설정됩 니다. 사이트 A에서 피어 IP 주소를 구성하는 경우 172.16.1.1로 변경해야 합니다. 원격단에 도 달할 수 있는 인터페이스도 지정됩니다. 클릭 Next 완료됩니다.

cha	Peer Device Identificat	on.	
. Introduction	This step lets you ident	ify the peer VPN device by its $\ensuremath{\mathbb{IP}}$ address and the interface used to access the peer.	
I. Peer Device Identification	Peer 1P Address:	192.168.1.1	
Traffic to protect	1991 Laura Tata Cara	(e-e-tale	
Security	VPIN Access Interface:	ontage .	
NAT Exempt			
Summary			

4. 로컬 및 원격 네트워크(트래픽 소스 및 대상)를 구성합니다. 이 그림에서는 사이트 B에 대한 컨 피그레이션을 보여줍니다(사이트 A에는 반대 방향이 적용됨).

Steps	Traffic to protect			
 Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary 	This step lets you i Local Network: Remote Network:	ientify the local network and remote network betwee 10.2.2.0_24 10.1.1.0_24	en which the traffic is to be protected using IPsec encryption.	
	< Back Ne	d>	Cancel	Help

5. Security(보안) 페이지에서 사전 공유 키를 구성합니다(양쪽 끝에서 일치해야 함). 클릭 Next 완 료됩니다.

Steps	Security
Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary	This step lets you secure the selected traffic. Simple Configuration ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer. Pre-shared Key: Customized Configuration You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.
	Center He

6. ASA에서 트래픽에 대한 소스 인터페이스를 구성합니다. ASDM은 ASA 버전을 기반으로 NAT(Network Address Translation) 규칙을 자동으로 생성하고 마지막 단계에서 나머지 컨피 그레이션과 함께 푸시합니다. **참고**: 이 문서에서 사용되는 예제의 경우 'inside'는 트래픽의 소 스입니다

1. Introduction This step allows you to exempt the local network addresses from network translation. 2. Peer Device Identification Image: Compt ASA side host/network from address translation image: Compt ASA sid	Steps	NAT Exempt	
	 Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summery 	This step allows you to exempt the local network addresses from network translation.	

7. 이제 마법사에서 ASA로 푸시되는 컨피그레이션의 요약을 제공합니다. 컨피그레이션 설정을 검토 및 확인한 다음 Finish.

Summary	
Brands Here is the summary of the configuration.	
Name	Value
Summary	
Peer Device IP Address	192.168.1.1
VPN Access Interface	outside
Protected Traffic	Local Network: 10.2.2.0/24 Remote Network: 10.1.1.0/24
IKE Version Allowed	IKE version 1 and IKE version 2
🖂 Authentication Method	
DKE v1	Use pre-shared key
DKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device
Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
E DKE v1	
IKE Policy	pre-share-aes-sha
IPsec Proposal	ESP-AE5-128-SHA, ESP-AE5-128-MD5, ESP-AE5-192-SHA, ESP-AE5-192-MD5 ESP-AE5-256-SHA, ESP-AE5-256-MD5, ESP-3DE5-SHA, ESP-3DE5-MD5, ESP-DE5-SHA, ESP-DE5-MD5
E DKE v2	
IKE Policy	
IPsec Proposal	AES256, AES192, AES, 3DES, DES

CLI를 통해 구성

이 섹션에서는 CLI를 통해 IKEv1 IPsec Site-to-Site 터널을 구성하는 방법에 대해 설명합니다.

ASA 버전 8.4 이상에 대해 사이트 B 구성

ASA 버전 8.4 이상에서는 IKEv1 및 IKEv2(Internet Key Exchange version 2)에 대한 지원이 도입되 었습니다.

팁: 두 버전 간의 차이점에 대한 자세한 내용은 ASA 8.4 코드 Cisco 문서의 IKEv1에서 IKEv2 L2L 터널로의 Swift Migration of IKEv1(IKEv2로 마이그레이션하는 <u>이유)</u> 섹션을 참조하십시 오.

팁: ASA의 IKEv2 컨피그레이션 예제를 보려면 ASA<u>와 라우터 컨피그레이션 예</u> Cisco 문서 사 이<u>의 Site-to-Site IKEv2 터널을</u> 살펴보십시오.

1단계(IKEv1)

1단계 컨피그레이션에 대해 다음 단계를 완료합니다.

1. 외부 인터페이스에서 IKEv1을 활성화하려면 CLI에 다음 명령을 입력합니다.

crypto ikev1 enable outside

2. 해싱, 인증, Diffie-Hellman 그룹, 수명 및 암호화에 사용할 알고리즘/방법을 정의하는 IKEv1 정 책을 생성합니다. authentication pre-share encryption aes hash sha group 2 lifetime 86400

3. IPsec 특성 아래에 터널 그룹을 만들고 피어 IP 주소 및 터널 사전 공유 키를 구성합니다.

tunnel-group 192.168.1.1 type ipsec-l2l tunnel-group 192.168.1.1 ipsec-attributes ikev1 pre-shared-key cisco ! Note the IKEv1 keyword at the beginning of the pre-shared-key command.

2단계(IPsec)

2단계 컨피그레이션에 대해 다음 단계를 완료합니다.

 암호화 및 터널링할 트래픽을 정의하는 액세스 목록을 만듭니다. 이 예에서 관심 트래픽은 10.2.2.0 서브넷에서 10.1.1.0으로 소스가 되는 터널의 트래픽입니다. 사이트 간에 여러 서브 넷이 포함된 경우 여러 항목을 포함할 수 있습니다.

버전 8.4 이상에서는 네트워크, 서브넷, 호스트 IP 주소 또는 여러 개체의 컨테이너 역할을 하는 개체 또는 개체 그룹을 만들 수 있습니다. 로컬 및 원격 서브넷이 있는 두 객체를 생성하여 암호화 ACL(Access Control List) 및 NAT 문 모두에 사용합니다.

object network 10.2.2.0_24 subnet 10.2.2.0 255.255.255.0 object network 10.1.1.0_24 subnet 10.1.1.0 255.255.255.0

access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24

2. TS(Transform Set)를 구성합니다. 이 설정에는 키워드가 포함되어야 합니다. IKEv1. 원격 엔드 에도 동일한 TS를 생성해야 합니다.

crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac

3. 다음 구성 요소가 포함된 암호화 맵을 구성합니다. 피어 IP 주소관심 트래픽을 포함하는 정의된 액세스 목록TS선택 사항인 PFS(Perfect Forward Secrecy) 설정 - 데이터를 보호하기 위해 사용되는 새로운 Diffie-Hellman 키 쌍을 생성합니다 (2단계가 시작되기 전에 양쪽이 PFS를 활성화해야 함).

4. 외부 인터페이스에 암호화 맵을 적용합니다.

crypto map outside_map 20 match address 100 crypto map outside_map 20 set peer 192.168.1.1 crypto map outside_map 20 set ikev1 transform-set myset crypto map outside_map 20 set pfs crypto map outside_map interface outside

NAT 예외

VPN 트래픽에 다른 NAT 규칙이 적용되지 않는지 확인합니다. 다음은 사용되는 NAT 규칙입니다.

nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static 10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup

참고: 여러 서브넷을 사용하는 경우 모든 소스 및 대상 서브넷을 포함하는 개체 그룹을 생성하 여 NAT 규칙에서 사용해야 합니다.

object-group network 10.x.x.x_SOURCE network-object 10.4.4.0 255.255.255.0 network-object 10.2.2.0 255.255.255.0

object network 10.x.x.x_DESTINATION network-object 10.3.3.0 255.255.255.0 network-object 10.1.1.0 255.255.255.0

nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE destination
static 10.x.x.x_DESTINATION 10.x.x.x_DESTINATION no-proxy-arp route-lookup

샘플 구성 완료

사이트 B의 전체 구성은 다음과 같습니다.

10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup

crypto ikev1 enable outside

crypto ikev1 policy 10 authentication pre-share encryption aes hash sha group 2 lifetime 86400 tunnel-group 192.168.1.1 type ipsec-121 tunnel-group 192.168.1.1 ipsec-attributes ikev1 pre-shared-key cisco !Note the IKEv1 keyword at the beginning of the pre-shared-key command. object network 10.2.2.0_24 subnet 10.2.2.0 255.255.255.0 object network 10.1.1.0_24 subnet 10.1.1.0 255.255.255.0 access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24 crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac crypto map outside_map 20 match address 100 crypto map outside_map 20 set peer 192.168.1.1 crypto map outside_map 20 set ikev1 transform-set myset crypto map outside_map 20 set pfs crypto map outside_map interface outside nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static

ASA 버전 8.2 이하에 대한 사이트 A 구성

이 섹션에서는 ASA 버전 8.2 이하에 대해 사이트 A를 구성하는 방법에 대해 설명합니다.

1단계(ISAKMP)

1단계 컨피그레이션에 대해 다음 단계를 완료합니다.

1. 외부 인터페이스에서 ISAKMP(Internet Security Association and Key Management Protocol)를 활성화하려면 CLI에 다음 명령을 입력합니다.

crypto isakmp enable outside **참고**: 여러 버전의 IKE(IKEv1 및 IKEv2)는 더 이상 지원되지 않으므로 1단계를 참조하기 위해 ISAKMP가 사용됩니다.

2. 1단계를 빌드하는 데 사용할 알고리즘/메서드를 정의하는 ISAKMP 정책을 만듭니다.

참고: 이 예제 컨피그레이션에서는 IKEv1 버전 9.x에서 다음으로 대체됨 ISAKMP. crypto isakmp policy 1 authentication pre-share encryption aes hash sha group 2 lifetime 86400

3. 사전 공유 키를 사용하여 피어 IP 주소(외부 IP 주소 5515)에 대한 터널 그룹을 생성합니다.

tunnel-group 172.16.1.1 type ipsec-121 tunnel-group 172.16.1.1 ipsec-attributes pre-shared-key cisco

2단계(IPsec)

2단계 컨피그레이션에 대해 다음 단계를 완료합니다.

 비전 9.x의 컨피그레이션과 마찬가지로, 원하는 트래픽을 정의하려면 확장 액세스 목록을 생 성해야 합니다.

access-list 100 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0

 사용 가능한 모든 암호화 및 해싱 알고리즘이 포함된 TS를 정의합니다(제공된 문제에는 물음 표가 있음). 다른 쪽에 구성된 것과 동일한지 확인합니다.

crypto ipsec transform-set myset esp-aes esp-sha-hmac

- 3. 다음 구성 요소를 포함하는 암호화 맵을 구성합니다. 피어 IP 주소관심 트래픽을 포함하는 정의된 액세스 목록TS데이터를 보호하기 위해 사용되는 새 Diffie-Hellman 키 쌍을 생성하는 PFS 설정(선택 사항). Phase 2가 시작되려면 양쪽이 PFS를 활성화해야 합니다.
- 4. 외부 인터페이스에 암호화 맵을 적용합니다.

```
crypto map outside_map 20 set peer 172.16.1.1
crypto map outside_map 20 match address 100
crypto map outside_map 20 set transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
```

NAT 예외

NAT 검사에서 제외할 트래픽을 정의하는 액세스 목록을 생성합니다. 이 버전에서는 해당 트래픽에 대해 정의한 액세스 목록과 비슷하게 표시됩니다.

access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 여러 서브넷을 사용하는 경우 동일한 액세스 목록에 다른 행을 추가합니다.

access-list nonat line 1 extended permit ip 10.3.3.0 255.255.255.0 10.4.4.0 255.255.255.0

액세스 목록은 다음과 같이 NAT와 함께 사용됩니다.

nat (inside) 0 access-list nonat

참고: 여기서 'inside'는 ASA가 액세스 목록과 일치하는 트래픽을 수신하는 내부 인터페이스의 이름을 나타냅니다.

샘플 구성 완료

사이트 A의 전체 구성은 다음과 같습니다.

```
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption aes
hash sha group 2
lifetime 86400
tunnel-group 172.16.1.1 type ipsec-121
tunnel-group 172.16.1.1 ipsec-attributes
pre-shared-key cisco
access-list 100 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
crypto ipsec transform-set myset esp-aes esp-sha-hmac
crypto map outside_map 20 set peer
crypto map outside_map 20 match address 100
crypto map outside_map 20 set transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
```

access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0

10.2.2.0 255.255.255.0

nat (inside) 0 access-list nonat

그룹 정책

그룹 정책은 터널에 적용되는 특정 설정을 정의하는 데 사용됩니다. 이러한 정책은 터널 그룹과 함 께 사용됩니다.

그룹 정책은 ASA에 정의된 특성에서 가져오는 internal 또는 외부 서버에서 쿼리하는 external로 정의할 수 있습니다. 그룹 정책을 정의하기 위해 사용되는 명령입니다.

group-policy SITE_A internal

참고: 그룹 정책에서 여러 특성을 정의할 수 있습니다. 가능한 모든 특성 목록은 Cisco ASA 5500 Series 버전 5.2의 Selected ASDM VPN Configuration Procedures의 <u>Configuring Group</u> <u>Policies</u> 섹션을 참조하십시오.

그룹 정책 선택적 특성

이 vpn-tunnel-protocol 특성은 이러한 설정을 적용해야 하는 터널 유형을 결정합니다. 이 예에서는 IPsec이 사용됩니다.

vpn-tunnel-protocol ?
group-policy mode commands/options:
IPSec IP Security Protocol l2tp-ipsec L2TP using IPSec for security
svc SSL VPN Client
webvpn WebVPN

vpn-tunnel-protocol ipsec - Versions 8.2 and prior vpn-tunnel-protocol ikev1 - Version 8.4 and later

터널을 구성하여 유휴 상태(트래픽 없음)를 유지하고 다운되지 않도록 할 수 있습니다. 이 옵션을 구 성하려면 vpn-idle-timeout 특성 값은 분을 사용해야 합니다. 그렇지 않으면 값을 none즉 터널이 절대 다 운되지 않습니다.

예를 들면 다음과 같습니다.

group-policy SITE_A attributes
vpn-idle-timeout ?
group-policy mode commands/options:
<1-35791394> Number of minutes
none IPsec VPN: Disable timeout and allow an unlimited idle period;

이 default-group-policy tunnel group의 general attributes 아래에 있는 명령은 설정된 터널에 대한 특정 정책 설정을 푸시하기 위해 사용되는 그룹 정책을 정의합니다. 그룹 정책에서 정의하지 않은 옵션 에 대한 기본 설정은 전역 기본 그룹 정책에서 가져옵니다. tunnel-group 172.16.1.1 general-attributes
default-group-policy SITE_A

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 이 섹션에 제공된 정보를 사용합니다.

ASDM

ASDM에서 터널 상태를 보려면 Monitoring > VPN. 제공되는 정보는 다음과 같습니다.

- 피어 IP 주소
- 터널을 구축하기 위해 사용되는 프로토콜
- 사용되는 암호화 알고리즘
- 터널이 가동된 시간과 가동 시간
- 수신 및 전송된 패킷 수입니다

팁: Refresh 최신 값을 보려면 데이터가 실시간으로 업데이트되지 않으므로

. 0 . ×	Charathering in VIII. In M	19 Statelles > Send								
Been # Covrect	1 C									
- 60	Pec		SSL VPN							-
15.130.53	Rameta	Site-to-Site	Clerites	With Client	Instite	Total	Enalmos	VPN Load Balancing	Total	Cursialitie
5.130.78	0.	1		0	0	0	. 0	0	1	1
5.130.107	Nor Ny: (Page Start	e Sile 🔶	Al Seattre	•						
* 100 III *	Connector Huffe	Protocol	Logn Time		ives to					1
edato.	10.5611	Diff Drive	12-16-16-17C Fe	Aprix 2015						6
VOLater Lowb	172.40.1.1	401-139	My Law Sta		191					1
September, Statutos norgalae, Statutos Ideal IVC, Prez, Statutos INC Sanater, Tuernary rotocol Statutos All Magging Sanatera letti SS, 1911 Servecturo, Statuto										
repression Statutos organian Statutos del IRA, Print Statutos C. Seastan Summary stocol Statutos Ali Magang Seastan em 55, 171 annestan Shajita										
represento Salantea Ingelano Salantea Sel IPC, Pere Statettea C Sanatero Sureneary theol Systems VII Nagang Sanatera es SS, IPN erectain Origina										
representor Salahtar upplen: Salahtar del IIC, Prez: Rataltar C. Baster Surmary Totol Salahtar MI Magang Salahtar MI Magang Salahtar MI Magang Salahtar MI Magang Salahtar MI Magang Salahtar										
Poentori Sarkito vysten Sarkito dei IPE (Phrs: Statistic Canadra Turner) thori Statistic Canadra Turner thori Statistic Magang Sanime et SS. (PR resolution Snight resolution Snight 1										
representor Sariatica registra: Sariatica del 1962 (Prez: Statettina Consento Russena (Escatetti Russena) (Escatetti Russena)										
epositori Sarkita optian Sarkita optian Sarkita Na PE Den: Statistic Caluaris Lavera Stoci Sarkita Sar	To art VPI assesses, to	git-tak ar The above to	die and select Table Sort O	tive from popular memo.						
Corporator Satata Nanyatar Stateta Robal III, Pres Satata Robal III, Pres Satata No Satata Satata Na Nagang Sasana Ani Nagang Sasana Kati Saging Carvesten Crapite										
powein Sahita wyke Sahita bi HC Phys Sahita bi HC Phys Sahita bi HC Phys Sahita bi Sahita Sahita Sahita Sahita Sahita Sahita Sahita Sahita Sahita Sahita Sah	To acr UNI amount, re	git cick on the above to	else and solic: 11.else Sort G	de fon pour neru.						

Combiew rate ata-1110	494394001				And the second s		10 X
File View Tools Weseds W	indov Help					vie kon b jondi	aluth.
😤 rone 🖓 Contgivetion [Manlong a Save Q Actest Q Sax	Orienard ? Http					CISCO
Device List Bookmarks	Confering > VII > 200 Statistics > Sensi	ana -					0
Devere Lief 2 5 ×							
Ade Dateta (P Cervant	Type	Active	Cumulative		Peek Concurrent	Inection	
THE 10,000,000 IN	Sta-to-Sta VPH		1		41	3	
-B 15 106 135 63			12		2 ¹	<u>_</u>	
- 8 15 105 126 70 - 8 15 105 136 R1							
D 10105130.002							
- 3 10 105 106 106 - 3 10 105 106 106	niter the Street	Al Seamers	. Ner				
ann 20	Correction His/Re Histord	Ligh Title	Bytes Tx				Details
82000	N2 36 11 851 854	2040 BUICHAP 10 JUIL	-10				Legist
- VPN Cluster Loads	102 SHILL BRANCESSE	Parc (-
Compression Statetics							the second se
Grind 32/Pres Switzley							
RAC Search Summary							
VLAN Mapping Develorer							
Clertine SS. VIV							
WSA Semirror							
and the second							
(Am)							
Conet Traffic Filler							
Part Pauling							
🚖 Tright Micro Content Security	To sart VPN assessore, sight clob on the above to	able and select Table Dort Order From popula intru-					
and Properties	ingout By - Al Sessions - +	Lignut Sessians					
12 vesto				- Refred			
200 B						2001	NAME OF BRIDE DOCUMENT
tara heheshed SuccessMin.					1800		H10/13 10/26 05 PH LTC

CLI

이 섹션에서는 CLI를 통해 컨피그레이션을 확인하는 방법에 대해 설명합니다.

1단계

사이트 B(5515) 측에서 1단계 컨피그레이션을 확인하려면 다음 명령을 CLI에 입력합니다.

show crypto ikev1 sa

Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: **192.168.1.1**

Type : L2L Role : **initiator** Rekey : no State : **MM_ACTIVE**

사이트 A(5510) 측에서 1단계 컨피그레이션을 확인하려면 다음 명령을 CLI에 입력합니다.

show crypto isakmp sa

Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1

1 IKE Peer: 172.16.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE

2단계

이 show crypto ipsec sa 명령은 피어 간에 구축된 IPsec SA를 표시합니다. 암호화된 터널은 네트워크 10.1.1.0과 10.2.2.0 간에 흐르는 트래픽에 대해 IP 주소 192.168.1.1과 172.16.1.1 사이에 구축됩니 다. 인바운드 및 아웃바운드 트래픽을 위해 구축된 2개의 ESP SA를 확인할 수 있습니다. AH(Authentication Header)는 AH SA가 없으므로 사용되지 않습니다.

사이트 B(5515) 측에서 2단계 컨피그레이션을 확인하려면 다음 명령을 CLI에 입력합니다.

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 172.16.1.1
local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
current_peer: 192.168.1.1
PERMIT, flags={origin_is_acl,}
#pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#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.: 172.16.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
     transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
      sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
     transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
      sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

사이트 A(5510) 측에서 2단계 컨피그레이션을 확인하려면 다음 명령을 CLI에 입력합니다.

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 192.168.1.1
    local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
    current_peer: 172.16.1.1
PERMIT, flags={origin_is_acl,}
    #pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#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.: 192.168.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
       transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
      transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

```
문제 해결
```

컨피그레이션 문제를 트러블슈팅하려면 이 섹션에 제공된 정보를 사용하십시오.

ASA 버전 8.4 이상

터널 실패의 위치를 확인하려면 다음 debug 명령을 입력합니다.

- debug crypto ikev1 127 (1단계)
- debug crypto ipsec 127 (2단계)

다음은 디버그 출력의 전체 예입니다.

```
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE Initiator: New Phase 1, Intf NP
Identity Ifc, IKE Peer 192.168.1.1 local Proxy Address 10.2.2.0, remote Proxy
Address 10.1.1.0, Crypto map (outside_map) Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing ISAKMP SA payload Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing NAT-Traversal VID ver 02 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver 03 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
```

```
ver RFC payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Fragmentation VID +
extended capabilities payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 172
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total
length : 132
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Oakley proposal is acceptable
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received NAT-Traversal ver 02 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Fragmentation VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, IKE Peer included IKE
fragmentation capability flags: Main Mode: True Aggressive Mode: True
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Cisco Unity
VID pavload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing xauth V6
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send IOS VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ISA_KE payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]?IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Cisco Unity client VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received xauth V6 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing VPN3000/ASA spoofing
IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Altiga/Cisco
VPN3000/Cisco ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Connection landed on tunnel_group
192.168.1.1
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, Generating
```

kevs for Initiator ... Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing ID payload Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, constructing hash pavload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing hash for ISAKMP Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing IOS keep alive payload: proposal=32767/32767 sec. 1 Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/10 ms ciscoasa# Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing dpd vid payload Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96 Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500 from 192.168.1.1:500 Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, ID_IPV4_ADDR ID received 192.168.1.1 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing hash payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing hash for ISAKMP Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing IOS keep alive payload: proposal=32767/32767 sec. Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing VID payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Received DPD VID Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Connection landed on tunnel_group 192.168.1.1 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Oakley begin quick mode Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator starting QM: msg id = 4c073b21 Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 1 COMPLETED Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Keep-alive type for this connection: DPD Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting P1 rekey timer: 73440 seconds. IPSEC: New embryonic SA created @ 0x75298588, SCB: 0x75C34F18, Direction: inbound SPI : 0x03FC9DB7 Session ID: 0x00004000 VPIF num : 0x0000002 Tunnel type: 121 Protocol : esp Lifetime : 240 seconds Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got SPI from key engine: SPI = 0x03fc9db7 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley constucting quick mode Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing blank hash payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

constructing IPSec SA payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing IPSec nonce payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing proxy ID Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Transmitting Proxy Id: Local subnet: 10.2.2.0 mask 255.255.255.0 Protocol 0 Port 0 Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0 Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending Initial Contact Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing qm hash payload Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending 1st QM pkt: msg id = 4c073b21 Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200 Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500 from 192.168.1.1:500 Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing hash payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing SA payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing nonce payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, ID_IPV4_ADDR_SUBNET ID received--10.2.2.0--255.255.255.0 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, loading all IPSEC SAs Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Generating Quick Mode Key! Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, NP encrypt rule look up for crypto map outside_map 20 matching ACL 100: returned cs_id=6ef246d0; encrypt_rule=752972d0; tunnelFlow_rule=75ac8020 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Generating Quick Mode Key! IPSEC: New embryonic SA created @ 0x6f0e03f0, SCB: 0x75B6DD00. Direction: outbound SPI : 0x1BA0C55C Session ID: 0x00004000 VPIF num : 0x0000002 Tunnel type: 121 Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0x1BA0C55C IPSEC: Creating outbound VPN context, SPI 0x1BA0C55C Flags: 0x0000005 SA : 0x6f0e03f0 SPI : 0x1BA0C55C MTU : 1500 bytes VCID : 0x0000000 Peer : 0x0000000

```
SCB : 0x0B47D387
Channel: 0x6ef0a5c0
IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0000f614
IPSEC: New outbound encrypt rule, SPI 0x1BA0C55C
Src addr: 10.2.2.0
Src mask: 255.255.255.0
Dst addr: 10.1.1.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x0000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x1BA0C55C
Rule ID: 0x74e1c558
IPSEC: New outbound permit rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x1BA0C55C
Rule ID: 0x6f0dec80
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, NP encrypt rule
look up for crypto map outside_map 20 matching ACL 100: returned cs_id=6ef246d0;
encrypt_rule=752972d0; tunnelFlow_rule=75ac8020
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Security negotiation
complete for LAN-to-LAN Group (192.168.1.1) Initiator, Inbound SPI = 0x03fc9db7,
Outbound SPI = 0x1ba0c55c
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley
constructing final quick mode
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator
sending 3rd QM pkt: msg id = 4c073b21
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=4c073b21)
with payloads : HDR + HASH (8) + NONE (0) total length : 76
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got a KEY_ADD
msg for SA: SPI = 0x1ba0c55c
IPSEC: New embryonic SA created @ 0x75298588,
SCB: 0x75C34F18,
Direction: inbound
SPI : 0x03FC9DB7
Session ID: 0x00004000
VPIF num : 0x0000002
Tunnel type: 121
Protocol : esp
```

Lifetime : 240 seconds IPSEC: Completed host IBSA update, SPI 0x03FC9DB7 IPSEC: Creating inbound VPN context, SPI 0x03FC9DB7 Flags: 0x0000006 SA : 0x75298588 SPI : 0x03FC9DB7 MTU : 0 bytes VCID : 0x0000000 Peer : 0x0000F614 SCB : 0x0B4707C7 Channel: 0x6ef0a5c0 IPSEC: Completed inbound VPN context, SPI 0x03FC9DB7 VPN handle: 0x00011f6c IPSEC: Updating outbound VPN context 0x0000F614, SPI 0x1BA0C55C Flags: 0x0000005 SA : 0x6f0e03f0 SPI : 0x1BA0C55C MTU : 1500 bytes VCID : 0x0000000 Peer : 0x00011F6C SCB : 0x0B47D387 Channel: 0x6ef0a5c0 IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C VPN handle: 0x0000f614 IPSEC: Completed outbound inner rule, SPI 0x1BA0C55C Rule ID: 0x74e1c558 IPSEC: Completed outbound outer SPD rule, SPI 0x1BA0C55C Rule ID: 0x6f0dec80 IPSEC: New inbound tunnel flow rule, SPI 0x03FC9DB7 Src addr: 10.1.1.0 Src mask: 255.255.255.0 Dst addr: 10.2.2.0 Dst mask: 255.255.255.0 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x0000000 Use SPI: false IPSEC: Completed inbound tunnel flow rule, SPI 0x03FC9DB7 Rule ID: 0x74e1b4a0 IPSEC: New inbound decrypt rule, SPI 0x03FC9DB7 Src addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x03FC9DB7 Use SPI: true

```
IPSEC: Completed inbound decrypt rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de830
IPSEC: New inbound permit rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPT: true
IPSEC: Completed inbound permit rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de8d8
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Pitcher:
received KEY_UPDATE, spi 0x3fc9db7
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting
P2 rekey timer: 24480 seconds.
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 2
COMPLETED (msgid=4c073b21)
```

ASA 버전 8.3 이전

터널 실패의 위치를 확인하려면 다음 debug 명령을 입력합니다.

```
• debug crypto isakmp 127 (1단계)
• debug crypto ipsec 127 (2단계)
```

다음은 디버그 출력의 전체 예입니다.

```
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
NONE (0) total length : 172
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Oakley proposal is acceptable
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 02 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 03 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal RFC VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Fragmentation VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE Peer included IKE fragmentation
capability flags: Main Mode: True Aggressive Mode: True
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing IKE SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE SA Proposal # 1, Transform # 1
acceptable Matches global IKE entry # 1
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ISAKMP SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Traversal VID ver
02 payload
```

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Fragmentation VID + extended capabilities payload Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 132 Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304 Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ke payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ISA_KE payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing nonce payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Cisco Unity client VID Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received xauth V6 VID Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing VPN3000/ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Altiga/Cisco VPN3000/Cisco ASA GW VID Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ke payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing nonce payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Cisco Unity VID payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing xauth V6 VID payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send IOS VID Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing VID payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send Altiga/Cisco VPN3000/Cisco ASA GW VID Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating keys for Responder... Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304 Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR ID received 172.16.1.1 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing hash for ISAKMP Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing IOS keep alive payload: proposal=32767/32767 sec. Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing VID pavload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Received DPD VID Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing ID payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing hash for ISAKMP Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing IOS keep alive payload: proposal=32767/32767 sec. Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing dpd vid payload Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96 Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 1 COMPLETED Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Keep-alive type for this connection: DPD Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P1 rekey timer: 82080 seconds. Feb 13 04:19:53 [IKEv1 DECODE]: IP = 172.16.1.1, IKE Responder starting QM: msg id = 4c073b21 Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing SA payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing nonce payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR_SUBNET ID received--10.2.2.0--255.255.255.0 Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received remote IP Proxy Subnet data in ID Payload: Address 10.2.2.0, Mask 255.255.255.0, Protocol 0, Port 0 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0 Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received local IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing notify payload Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, QM IsRekeyed old sa not found by addr Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map check, checking map = outside_map, seg = 20... Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map check, map outside_map, seq = 20 is a successful match Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Remote Peer configured for crypto map: outside_map Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing IPSec SA payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IPSec SA Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20 Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE: requesting SPI! IPSEC: New embryonic SA created @ 0xAB5C63A8, SCB: 0xABD54E98, Direction: inbound SPI : 0x1BA0C55C Session ID: 0x00004000 VPIF num : 0x0000001 Tunnel type: 121

Protocol : esp Lifetime : 240 seconds Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got SPI from key engine: SPI = 0x1ba0c55c Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, oakley constucting quick mode Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing blank hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing IPSec SA payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing IPSec nonce pavload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing proxy ID Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Transmitting Proxv Id: Remote subnet: 10.2.2.0 Mask 255.255.255.0 Protocol 0 Port 0 Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing qm hash payload Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Responder sending 2nd QM pkt: msg id = 4c073b21 Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172 Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 52 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, loading all TPSEC SAS Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating Quick Mode Key! Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule look up for crypto map outside_map 20 matching ACL 100: returned cs_id=ab9302f0; rule=ab9309b0 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating Quick Mode Key! IPSEC: New embryonic SA created @ 0xAB570B58, SCB: 0xABD55378, Direction: outbound SPT : 0x03FC9DB7 Session ID: 0x00004000 VPIF num : 0x0000001 Tunnel type: 121 Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0x03FC9DB7 IPSEC: Creating outbound VPN context, SPI 0x03FC9DB7 Flags: 0x0000005 SA : 0xAB570B58 SPI : 0x03FC9DB7 MTU : 1500 bytes VCID : 0x0000000 Peer : 0x0000000 SCB : 0x01512E71 Channel: 0xA7A98400 IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7 VPN handle: 0x0000F99C IPSEC: New outbound encrypt rule, SPI 0x03FC9DB7 Src addr: 10.1.1.0 Src mask: 255.255.255.0 Dst addr: 10.2.2.0 Dst mask: 255.255.255.0

```
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x0000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x03FC9DB7
Rule ID: 0xABD557B0
IPSEC: New outbound permit rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x03FC9DB7
Rule ID: 0xABD55848
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule
look up for crypto map outside_map 20 matching ACL 100: returned cs_id=ab9302f0;
rule=ab9309b0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Security negotiation
complete for LAN-to-LAN Group (172.16.1.1) Responder, Inbound SPI = 0x1ba0c55c,
Outbound SPI = 0x03fc9db7
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got a
KEY_ADD msg for SA: SPI = 0x03fc9db7
IPSEC: Completed host IBSA update, SPI 0x1BA0C55C
IPSEC: Creating inbound VPN context, SPI 0x1BA0C55C
Flags: 0x0000006
SA : 0xAB5C63A8
SPI : 0x1BA0C55C
MTU : 0 bytes
VCID : 0x0000000
Peer : 0x0000F99C
SCB : 0x0150B419
Channel: 0xA7A98400
IPSEC: Completed inbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0001169C
IPSEC: Updating outbound VPN context 0x0000F99C, SPI 0x03FC9DB7
Flags: 0x0000005
SA : 0xAB570B58
SPI : 0x03FC9DB7
MTU : 1500 bytes
VCID : 0x0000000
Peer : 0x0001169C
SCB : 0x01512E71
Channel: 0xA7A98400
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x0000F99C
```

```
IPSEC: Completed outbound inner rule, SPI 0x03FC9DB7
Rule ID: 0xABD557B0
IPSEC: Completed outbound outer SPD rule, SPI 0x03FC9DB7
Rule ID: 0xABD55848
IPSEC: New inbound tunnel flow rule, SPI 0x1BA0C55C
Src addr: 10.2.2.0
Src mask: 255.255.255.0
Dst addr: 10.1.1.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x0000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x1BA0C55C
Rule ID: 0xAB8D98A8
IPSEC: New inbound decrypt rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x1BA0C55C
Rule ID: 0xABD55CB0
IPSEC: New inbound permit rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x1BA0C55C
Rule ID: 0xABD55D48
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Pitcher: received
KEY_UPDATE, spi 0x1ba0c55c
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P2 rekey
```

timer: 27360 seconds.
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 2 COMPLETED
(msgid=4c073b21)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.