Cisco IOS/CCP - Cisco CP로 DMVPN 구성

목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 표기 규칙 배경 정보 구성 네트워크 다이어그램 Cisco CP를 사용한 스포크 구성 스포크에 대한 CLI 컨피그레이션 Cisco CP를 사용한 허브 컨피그레이션 허브에 대한 CLI 컨피그레이션 CCP를 사용하여 DMVPN 컨피그레이션 수정 추가 정보 다음을 확인합니다. 관련 정보

<u>소개</u>

이 문서에서는 Cisco CP(Configuration Professional)를 사용하여 허브와 스포크 라우터 간 DMVPN(Dynamic Multipoint VPN) 터널의 샘플 컨피그레이션을 제공합니다. Dynamic Multipoint VPN은 GRE, IPSec 암호화, NHRP 및 라우팅과 같은 다양한 개념을 통합하여 최종 사용자가 동적 으로 생성된 스포크 투 스포크 IPSec 터널을 통해 효과적으로 통신할 수 있는 정교한 솔루션을 제공 하는 기술입니다.

<u>사전 요구 사항</u>

<u>요구 사항</u>

최상의 DMVPN 기능을 위해서는 Cisco IOS® Software Release 12.4 메인라인 12.4T 이상을 실행 하는 것이 좋습니다.

<u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Router 3800 Series with Software 릴리스 12.4(22)
- Cisco IOS Router 1800 Series with Software 릴리스 12.3(8)

• Cisco Configuration Professional 버전 2.5

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.

<u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 규칙</u>을 참조하십시오.

<u>배경 정보</u>

이 문서에서는 Cisco CP를 사용하여 라우터를 스포크로 구성하고 다른 라우터를 허브로 구성하는 방법에 대해 설명합니다. 초기 스포크 컨피그레이션이 표시되지만, 이 문서의 뒷부분에는 허브 관 련 컨피그레이션이 자세히 표시되어 더 잘 이해할 수 있습니다. 허브에 연결하기 위해 유사한 접근 방식을 사용하여 다른 스포크를 구성할 수도 있습니다. 현재 시나리오는 다음 매개변수를 사용합니 다.

- 허브 라우터 공용 네트워크 209.165.201.0
- 터널 네트워크 192.168.10.0
- 사용된 라우팅 프로토콜 OSPF

<u>구성</u>

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: <u>명령 조회 도구(등록된</u> 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

<u>네트워크 다이어그램</u>

이 문서에서는 다음 네트워크 설정을 사용합니다.



Cisco CP를 사용한 스포크 구성

이 섹션에서는 Cisco Configuration Professional에서 단계별 DMVPN 마법사를 사용하여 라우터를 스포크로 구성하는 방법을 보여줍니다.

 1. Cisco CP 애플리케이션을 시작하고 DMVPN 마법사를 시작하려면 Configure(구성) >

 Security(보안) > VPN > Dynamic Multipoint VPN(동적 멀티포인트 VPN)으로 이동합니다. 그

 런 다음 DMVPN에서 스포크 생성 옵션을 선택하고 선택한 작업 시작 을 클릭합니다

VPN	
reate Dynamic Multipoint VPN (DMVPN) Edit Dynamic Multipoint VPN (DMVPN)	
Configure DMVPN Spoke	
e theread	
Spoke 1 Clast	
Sooke 2	
Create a spoke (client) in a DMVPH	
Use this option to configure the router as a spoke in a full mesh or hub	
and spoke network topology. To complete this configuration, you must	
policy, IPSec Transform set and dynamic routing protocol information.	
C Create a hub (server or head-end) in a DMVPN	
Create a hub (server or head-end) in a DMVPN Use this option to configure the router as a primary or backup hub. If you	
Create a hub (server or head-end) in a DMVPN Use this option to configure the router as a primary or backup hub. If you are configuring a backup hub, you must know the primary hub's NHRP	
Create a hub (server or head-end) in a DMVPN Use this option to configure the router as a primary or backup hub. If you are configuring a backup hub, you must know the primary hub's NHRP information, pre-shared key, IKE policy, IPSec Transform set and dynamic routing protocol information.	
Create a hub (server or head-end) in a DMVPN Use this option to configure the router as a primary or backup hub. If you are configuring a backup hub, you must know the primary hub's NHRP information, pre-shared key, IKE policy, IPSec Transform set and dynamic routing protocol information.	
Create a hub (server or head-end) in a DMVPN Use this option to configure the router as a primary or backup hub. If you are configuring a backup hub, you must know the primary hub's NHRP information, pre-shared key, IKE policy, IPSec Transform set and dynamic routing protocol information.	
Create a hub (server or head-end) in a DMVPN Use this option to configure the router as a primary or backup hub. If you are configuring a backup hub, you must know the primary hub's NHRP information, pre-shared key, IKE policy, IPSec Transform set and dynamic routing protocol information.	

2. Next(다음)를 클릭하여 시작합니다

DMVPN Spoke Wizard	
VPN Wizard	Configure a DMVPN spoke
	DMVPN allows you to create a scalable network that connects multiple remote routers to a central hub router using the same security features offered by site-to-site VPNs. DMVPN uses IPSec, NHRP, GRE and routing protocols to create secure tunnels between a hub and a spoke. This wizard allows you to configure the router as a DMVPN spoke. The wizard guides you through these tasks: * Specifying the DMVPN network topology. * Providing hub information. * Configuring a GRE tunnel interface. * Configuring a gre-shared key. * Configuring an IPSec transform set. * Configuring a dynamic routing protocol. To begin, click Next.
	Back Next > Finish Cancel Help

3. Hub and Spoke 네트워크 옵션을 선택하고 Next를 클릭합니다



4. 허브 라우터의 공용 인터페이스 및 허브 라우터의 터널 인터페이스와 같은 허브 관련 정보를 지정합니다

DMVPN Spoke Wizard (Ht	ib and Spoke Topology) - 20% Complete		×
VPN Wizard	Specify Hub Information Enter the IP address of the hub and the IP addre Contact your network administrator to get this in	ess of the hub's mGRE tunnel interface. formation.	
	Hub Information		
	IP address of hub's physical interface.	209.165.201.2	
	IP address of hub's mGRE tunnel interface:	192.168.10.2	
	Spoke You are configuring this spoke router Bit is spoke router Bi	Iblic IP address be entered above Hub RE tunnel	
	<	Back Next > Finish Cancel H	lelp

5. 스포크의 터널 인터페이스 세부 정보 및 스포크의 공용 인터페이스를 지정합니다. 그런 다음 Advanced(고급)를 클릭합니다

		1		100
Select the interface that connect	is to the Inte	met: L	FastEthernet0	
A Selecting an interface config be always up.	ured for a d	ialup connectio	n may cause the cor	nnection t
GRE Tunnel Interface				
A GRE tunnel interface will be address information for this in	created for terface.	this DMVPN co	nnection. Please ent	ler the
IP address of the tunnel in	nterface —	Advanced	settings	
IP Address:		Click Advance	ed to verify that value	s
192.168.10.5		match peer s	ettings.	
Subnet Mask:			Advan	ced
255.255.255.0	24		\sim	
Interface connected to Internet. This is the interface from which GRE/mGRE Tunnel originaties- Internet	Logic IP ad interf in the For n help	al GRE/mGRE Tu dress of GRE/mGi ace on all hubs an rivate IP addresse is ame subnet. nore information pl button.	nnel interface. RE tunnel d spoke routers s and must be ease click the	

6. 터널 <u>매개변수 및 NHRP 매개변수를 확인하고 허브 매</u>개변수와 완벽하게 일치하는지 확인합

from your network administrator I Cisco CP defaults.	before changin
NHRP NHRP Authentication String:	DMVPN_NW
NHRP Network ID:	100000
NHRP Hold Time:	360
GRE Tunnel Interface Inform	nation
Bandwidth:	100000
MTU:	1400
Tunnel Throughput Delay:	1000

7. 사전 공유 키를 지정하고 Next(*다음*)를 클릭합니다

DMVPN Spoke Wizard (Hi	ub and Spoke Topology) - 40% Complete		×
	Authentication Select the method you DMVPN network. You o the router must have a on this router must ma C Digital Certificate (C Pre-shared Keys pre-shared key: Reenter key:	want to use to authenticate an use digital certificate or valid certificate configured. Ich the keys configured on s	this router to the peer devic a pre-shared key. If digital co If pre-shared key is used, th all other routers in the DMVF	e(s) in the ertificate is used, le key configured 'N network.
		< Ba	ack Next Finish Ca	ncel Help

8. 별도의 IKE 제안을 추가하려면 Add를 클릭합니다

DMVPN Spoke Wizard (Hub and Spoke Topology) - 50% Complete

VPN Wizard

IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

a la sur a sur		Priority	Encryption	Hash	D-H Group	Authentication	Туре
	1	1	3DES	SHA_1	group2	PRE_SHARE	Cisco CP Defa
1 and							
1 -							
		ud)	Edit	Ĩ.			
A Description	Ľ		Legino.				
and a second sec							
ST PA							

9. 암호화, 인증 및 해시 매개변수를 지정합니다. 그런 다음 확인을 클릭합니다

Priority:	Authentication:
2	PRE_SHARE
Encryption:	D-H Group:
AES_192 🛃	group1
lash:	Lifetime:
SHA_1 🛛 🗹	24 0 0 HH:MM:SS

10. 새로 생성된 IKE 정책은 여기에서 확인할 수 있습니다. Next(*다음)를 클릭합니다*

PN Wizard	IKE	Proposals proposals	specify the en	cryption algo	rithm, authenticat	ion algorithm an	d key exchange
	meth	nod that is	used by this r VPN connecti	outer when n	egotiating a VPN blished with the r	connection with t	he remote
	devi	ce should l	be configured	with at least	one of the policie	s listed below.	
	Clic	k the Add	button to add	t more policie	as and the Edit	outton to edit an e	existing policy
		Priority	Encryption	Hash	D-H Group	Authentication	Туре
10 Albert			3DES	SHA_1	group2	PRE_SHARE	Cisco CP Def
		2	AE5_192	SHA_1	groupi	PRE_SHARE	OserDelined
	2						
	15						
				1			
a second		Add	Edit				
1 and	2		-	-			
and the second							
and the second s	100						

11. Next(*다음*)를 클릭하여 기본 변형 집합을 계속 진행합니다

VPN Wizard	Transfe	orm Set form est enseifies #	a encountion and out	hantication algorit	one used to protect th
	data in t	the VPN tunnel. Sin	ce the two devices m	ust use the same	algorithms to
	commu	nicate, the remote	device must be config	ured with the sam	e transform set as the
	one sel	ected below.			
\sim	Click the	e Add button to ac	id a new transform se	and the Edit bu	tton to edit the specifi
	transfor	m set.			
	Select.	Transform Set			
	Select	manalonni oel.			
12715		Cisco CP Default Tr	ansform Set 🔜 💌 🗆		
	Deta	ails of the specified	transform set		
		Name	ESP Encryption	ESP Integrity	AH Integrity
		ESP-3DES-SHA	ESP 3DES	ESP SHA HMAC	1 a consegura
	-				
la					
A BARRIER					10
Ref &		1	-1		2.5
	1	Add Edit			

12. 필요한 라우팅 프로토콜을 선택합니다. 여기서 OSPF가 선택됩니다

DMVPN Spoke Wizard (Hu	b and Spoke Topology) - 70% Complete	×
VPN Wizard	Select Routing Protocol Routing protocols are used to advertise private networks behind this router to other routers in the DMVPN. Select the dynamic routing protocol you want to use. Note: You can only create as many OSPF processes as the number of interfaces that are configured with an IP address and have the status administratively up.	
	Back Next > Finish Cancel Help	p

13. OSPF 프로세스 ID 및 영역 ID를 지정합니다. OSPF에서 알릴 네트워크를 추가하려면 Add를 클릭합니다

PN Wizard	Routing Information	on		
	C Select an existi	ing OSPF process ID	<u></u>	
	Create a new C	OSPF process ID:	(1	0)
- A	OSPF Area ID for	tunnel network:	2	
A	Add the private net must be enabled of	tworks that you want i on the other routers t rks advertised using	to advertise to the other o send and receive thes OSPF	r routers in this DMVF se advertisements.
	Network	Wildcard Mask	Area	Add
				Edit
				Delete
	Private Networ advertised to the	rk that will be the DMVPN cloud.		
	Private Networ advertised to the Internet	rk that will be the DMVPN cloud.	< Back Next >	Finish
	Private Networ advertised to the UMVPN Cloud	rk that will be the DMVPN cloud.	< Back Next > Add a Network	Finish Cancel
	Private Networ advertised to the Internet DMVPN Cloud	rk that will be the DMVPN cloud.	< Back Next > Add a Network Network:	Finish Cancel
	Private Networ advertised to the Internet DMVPN Cloud	rk that will be the DMVPN cloud.	< Back Next > Add a Network Network: Wildcard Mask:	Finish Cancel 192.168.10.0 0.0.0.255
	Private Networ advertised to the Internet DMVPN Cloud	rk that will be the DMVPN cloud.	< Back Next > Add a Network Network: Wildcard Mask:	Finish Cancel 192.168.10.0 0.0.255
	Private Networ advertised to the Internet DMVPN Cloud	rk that will be the DMVPN cloud.	< Back Next > Add a Network Network: Wildcard Mask: Area:	Finish Cancel 192.168.10.0 0.0.0.255 2
	Private Networ advertised to the DMVPN	rk that will be the DMVPN cloud.	< Back Next > Add a Network Network: Wildcard Mask Area:	Einish Cancel

zard Routing Information	Routing Information					
C Select an existing	OSPF process ID					
Create a new OSI	PF process ID:		10			
OSPF Area ID for tur	inel network:		2			
Add the private networks	orks that you want i the other routers to advertised using	to advertise to t o send and rec OSPF	the other routers in this C eive these advertisemen			
Network	Wildcard Mask	Area	Add			
192.168.10.0 172.16.18.0	0.0.0.255 0.0.0.255	2 2	Edit Delete			
Private Network th advertised to the f	nat will be DMVPN cloud.					
	1					

16. *마침*을 클릭하여 마법사 구성을 완료합니다



17. Deliver(*전달*)를 클릭하여 명령을 실행합니다. 컨피그레이션을 저장하려면 Save running config to device's startup config 확인란을 선택합니다

Deliver Configuration to Device	
Deliver delta commands to the device's running config.	
Preview commands that will be delivered to the device's running configuration	1.
crypto ipsec transform-set ESP-3DES-SHA esp-sha-hinac esp-3des mode transport exit crypto ipsec profile CiscoCP_Profile1	
set transform-set ESP-3DES-SHA exit interface Tunnel0	
ext	
default interface Tunnel0 interface Tunnel0	
hendwidth 1000	×
1	2
The differences between the running configuration and the startu the device is turned off.	p configuration are lost whenever
Save running config. to device's startup config. This operation can take several minutes.	
Deliver Cancel Save to file	Help

<u>스포크에 대한 CLI 컨피그레이션</u>

관련 CLI 컨피그레이션은 다음과 같습니다.

스포크 라우터

```
crypto ipsec transform-set ESP-3DES-SHA esp-sha-hmac
esp-3des
mode transport
exit
crypto ipsec profile CiscoCP_Profile1
set transform-set ESP-3DES-SHA
exit
interface Tunnel0
exit
default interface Tunnel0
interface Tunnel0
bandwidth 1000
delay 1000
ip nhrp holdtime 360
ip nhrp network-id 100000
ip nhrp authentication DMVPN_NW
ip ospf network point-to-multipoint
ip mtu 1400
no shutdown
ip address 192.168.10.5 255.255.255.0
ip tcp adjust-mss 1360
ip nhrp nhs 192.168.10.2
ip nhrp map 192.168.10.2 209.165.201.2
tunnel source FastEthernet0
tunnel destination 209.165.201.2
tunnel protection ipsec profile CiscoCP_Profile1
tunnel key 100000
exit
router ospf 10
network 192.168.10.0 0.0.0.255 area 2
network 172.16.18.0 0.0.0.255 area 2
exit
crypto isakmp key ******* address 209.165.201.2
crypto isakmp policy 2
authentication pre-share
encr aes 192
hash sha
group 1
lifetime 86400
exit
crypto isakmp policy 1
authentication pre-share
encr 3des
hash sha
group 2
lifetime 86400
exit
```

Cisco CP를 사용한 허브 컨피그레이션

이 섹션에서는 DMVPN에 대한 허브 라우터를 구성하는 방법에 대한 단계별 접근 방식을 보여줍니 다. 1. Configure(구성) *> Security(보안) > VPN > Dynamic Multipoint VPN*으로 이동하고 Create a *hub in a DMVPN* 옵션*을* 선택합니다. 에서 *선택한 작업 시작을* 클릭합니다

eate Dynamic Multipoint VPN (DMVPN)	Edit Dynamic Multipoint VPN (DMVPN)
Create a spoke (client) in a DMVPN Use this option to configure the rou and spoke network topology. To con know the hub's IP address, NHRP i policy, IPSec Transform set and dyn	ter as a spoke in a full mesh or hub mplete this configuration, you must information, pre-shared key, IKE namic routing protocol information.
Create a hub (server or head-end) in	a DMVPN
Lice this option to configure the rou	ter as a primary or backup hub. If you

2. Next(*다음)를 클릭합니다*

DMVPN Hub Wizard	
VPN Wizard	Configure a BMVPN hub
	DMVPN allows you to create a scalable network that connects multiple remote routers to a contrain hub router using the same security features offered by site-to-site VPNs. DMVPN uses IPSec, NHRP, GRE and routing protocols to create secure tunnels between a hub and a spoke. This wizard allows you to configure the router as a DMVPN hub. The wizard guides you through these tasks: * Specifying the DMVPN network topology. * Specifying the hub type. * Configuring a multipoint GRE tunnel. * Configuring an PISec transform set. * Configuring an IPSec transform set. * Configuring a dynamic routing protocol. To begin, click Next
	Back Next> Finish Cancel Help
Linh and Charles IIIE	- 이그 오셔요 서태된 그 May 4를 크리하니다

3. Hub and Spoke 네트워크 옵션을 선택하고 Next를 클릭합니다



4. 기본 허브를 선택합니다. 그런 다음 다음을 클릭합니다

VPN Wizard	Type of Hub In a DMVPN network there will be a hub router and multiple spoke routers connecting to the hub. You can also configure multiple routers as hubs. The additional routers will act as backups. Select the type of hub you want to configure this router as.
	Primary hub
	C Backup Hub(Cisco CP does not support backup hub configuration on this router)
NF	
	< Back Next > Finish Cancel Help

5. Tunnel 인터페이스 매개변수를 지정하고 Advanced(고급)를 클릭합니다

VPN Wizard	Multipoint GRE Tunnel Interface Co	nfigura	tion				
ee, oo oo oo oo oo oo oo	Select the interface that connects to	the Inte	emet:	GigabitEthernet0/0	*		
	A Selecting an interface configured be always up.	l for a d	ialup conne	ction may cause the conn	ection		
	Multi point GRE (mGRE) Tunne	Interfa	ce				
	A GRE tunnel interface will be crea	ated for	this DMVPN	I connection. Please enter	the		
	address information for this interfa	ice.					
	IP address of the tunnel interf	ace —	Advan	ced settings			
and the	IP Address:		Click Adv	anced to verify that values			
	192.168.10.2	192.168.10.2			match peer settings.		
	Subnet Mask:			Advance	d		
n 🔨 🚘	255.255.255.0 2	4					
		Locit	al GRE/mGRI	F Turmel interface			
-		IP ad	dress of GRE	mGRE tunnel			
	Interface connected to Internet.	are p	rivate IP addre	esses and must be			
	GRE/mGRE Tunnel originaties-	For n help	nore informatio button.	on please click the			
State of the second second	Internet	100					

6. Tunnel(터널) 매개변수 및 NHRP 매개변수를 지정합니다. 그런 다음 *확인*을 클릭합니다

Advanced configuration for the tunnel inter... 🔀

Some of the following parameters should be identical in all devices in this DMVPN. Obtain the correct values from your network administrator before changing the Cisco CP defaults.

NHAP Autientication ounig.	DMVPN_NW
NHRP Network ID:	100000
IHRP Hold Time:	360
unner rvey.	100000
Funnel Kev	100000
	the second se
Bandwidth:	1000
Bandwidth: MTU:	1000

7. 네트워크 설정에 따라 옵션을 지정합니다



8. 사전 공유 키를 선택하고 사전 공유 키를 지정합니다. 그런 다음 다음을 클릭합니다

DMVPN Hub Wizard (Hub	and Spoke Topology) -	40% Complete		X
VPN Hub Wizard (Hub	Authentication Select the method you w DMVPN network. You ca the router must have a v on this router must mate C Digital Certificates Pre-shared Keys pre-shared key: Reenter key:	40% Complete vant to use to auth n use digital certi- alid certificate cor th the keys config	enticate this router to the peer d ficate or a pre-shared key. If digit ifigured. If pre-shared key is use ured on all other routers in the D	evice(s) in the tal certificate is used, d, the key configured
			< Back (Next >) Finish	Cancel Help

9. 별도의 IKE 제안을 추가하려면 Add를 클릭합니다

DMVPN Hub Wizard (Hub and Spoke Topology) - 50% Complete

VPN Wizard

SHA_1

0K

IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

	Priority Encryption I 3DES Add Edit.	Hash SHA_1	D-H Group group2	Authentication PRE_SHARE	Type Cisco CP Defat
			< Back Nex	t> Finish C	Cancel Help
10. 암호화, 인증 및 해시 [배개변수를 지정합니디	h. 그런 다음	음 <i>확인</i> 을 클	릭합니다	
Add IKE Policy					
Configure IKE Policy	4		-		
Priority:	Authentication:				
2	PRE_SHARE	~			
Encryption:	D-H Group:				
AES_192	group1	~			
Hash:	Lifetime:				

11. 새로 생성된 IKE 정책은 여기에서 확인할 수 있습니다. Next(*다음)를 클릭합니다*

0

0

Help

HH:MM:SS

24

Cancel

DMVPN Hub Wizard (Hub and Spoke Topology) - 50% Complete

DMVPN Hub Wizard (Hu
VPN Wizard

IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

1.1	Priority	Encryption	Hash	D-H Group	Authentication	Туре
	1 2	3DES AES_192	SHA_1 SHA_1	group2 group1	PRE_SHARE PRE_SHARE	Cisco CP Def User Defined
1		11. 7	1			
	Add	Edit.				
	Add	Edit				

12. Next(*다음*)를 클릭하여 기본 변형 집합을 계속 진행합니다

VPN Wizard	A transform Set A transform set spec data in the VPN tunnic communicate, the re one selected below.	ifies the encryption and el. Since the two devices mote device must be co	authentication algorit s must use the same nfigured with the sam	hms used to protect the algorithms to ne transform set as the
	Click the Add buttor transform set. Select Transform Se	n to add a new transforn t:	n set and the Edit bu	atton to edit the specifie
St.S.	Cisco CP Defa	ault Transform Set 🛛 🛓		
	Details of the spe	cified transform set		
	Name	ESP Encrypt	ion ESP Integrity	AH Integrity
KE	as ESP-3DES-	50A ESP_3DES.	ESP_SHA_HMA	
	Add	Edit		3

13. 필요한 라우팅 프로토콜을 선택합니다. 여기서 OSPF가 선택됩니다

VPN Wizard	Select Routing Protocol Routing protocols are used to advertise private networks behind this router to other routers in the DMVPN. Select the dynamic routing protocol you want to use. Note: You can only create as many OSPF processes as the number of interfaces that are configured with an IP address and have the status administratively up.
Re	
	< Back Next > Finish Cancel Help

14. OSPF 프로세스 ID 및 영역 ID를 지정합니다. OSPF에서 알릴 네트워크를 추가하려면 Add를 클릭합니다

VPN Wizard	Routing Informati	ion		
	C Select an exist	ing OSPF process ID.		×
	Create a new (OSPF process ID:	ſ	10
	OSPF Area ID for	tunnel network:	Į	2
all'	Add the private ne must be enabled	tworks that you want i on the other routers to rks advertised using	to advertise to the o o send and receive OSPF	ther routers in this DMVPI these advertisements.
	Network	Wildcard Mask	Area	(bbb
	Private Netwo	rk that will be		
	Private Networksed for the advertised for the adver	rk that will be he DMIVPN cloud.		
	Private Networksed for the advertised for the adver	rk that will be he DMVPN cloud.	< Back Ne	xt > Finish Cancel
	Private Networksed for advertised for a	rk that will be he DMVPN cloud.	< Back Ne Add a Network	xt > Finish Cancel
	Private Networksed for advertised for a	rk that will be he DMVPN cloud.	< Back Ne Add a Network Network:	xt > Finish Cancel 192.168.10.0
	Private Networksed for advertised for a	rk that will be he DMVPN cloud.	< Back Ne Add a Network Network:	xt > Finish Cancel 192.168.10.0
	Private Networksed for advertised for a	rk that will be he DMVPN cloud.	 Back Ne Add a Network Network: Wildcard Mask 	xt > Finish Cancel 192.168.10.0 0.0.0.255
	Private Networksed for advertised fo	rk that will be he DMVPN cloud.	 Back Ne Add a Network Network: Wildcard Mask Area: 	xt > Finish Cancel 192.168.10.0 0.0.0.255 2

16. 허브 라우터 뒤에 프라이빗 네트워크를 추가하고 Next(다음)를 클릭합니다

Wizard	Routing Informatio	n		
and the second s	C Select an existin	ig OSPF process ID		35
	(F Create a new Of	SPF process ID:		10
-	OSPF Area ID for funnel network:			2
all and a second	must be enabled o	n the other routers t ks advertised using	o send and red	eive these advertisements.
	Network	Wildcard Mask	Area	Add.
	192.168.10.0 172.16.20.0	0.0.0.255 0.0.0.255	2	East.
JE	Private Network	that will be o DMVPN cloud.		

17. *마침*을 클릭하여 마법사 구성을 완료합니다



18. Deliver(*전달*)를 클릭하여 명령을 실행합니다

Giver deite Comme	us to the devices	s rouning contrig.		
review commands	hat will be deliver	red to the device's r	unning configuration.	
rypto keyring cop-o	mypn-keyring			1.3
pre-shared-key add	ress 0.0.0.0 0.0.0	0.0 key *******		
exe transfr	muset ESP. 3DES.	SHå esn sha hma	esn_3des	
mode transport	11-301 201 -0020-	-ora- cop-ora-rinto	a cala-adea	
exit				
rypto isakmp profile	ccp-dmvpn-isakr	nprofile		
keyring ccp-dmvpn-	keyring			
exit	55 0.0 0 0			
vunto incor nintilo	"iona"D Drafilat			
				2
sxit Kunto insec profile C	"ionn"D Drofilat			

<u>허브에 대한 CLI 컨피그레이션</u>

관련 CLI 컨피그레이션은 다음과 같습니다.

허브 라우터
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp policy 2
encr aes 192
authentication pre-snare
crypto isakiip key abcuizs address 0.0.0.0 0.0.0.0
crvpto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac
mode transport
!
crypto ipsec profile CiscoCP_Profile1
set transform-set ESP-3DES-SHA
!
interface TunnelO
bandwidth 1000
ip address 192.168.10.2 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication DMVPN_NW
ip nhrp map multicast dynamic
ip nhrp holdtime 360

```
ip tcp adjust-mss 1360
ip ospf network point-to-multipoint
delay 1000
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile CiscoCP_Profile1
!
router ospf 10
log-adjacency-changes
network 172.16.20.0 0.0.0.255 area 2
network 192.168.10.0 0.0.0.255 area 2
```

CCP를 사용하여 DMVPN 컨피그레이션 수정

터널 인터페이스를 선택하고 Edit(수정)를 클릭할 때 기존 DMVPN 터널 매개변수를 수동으로 편집 할 수 *있습니다*.

VPN			
reate Dynamic Multip	oint VPN (DMVPN) Edit Dynam	ic Multipoint VPN (DMVPN)	
	1.0.000		Add Edit Dele
Interface	IPSec Profile	IP Address	Description
Funnel0	CiscoCP_Profile1	192.168.10.2	<none></none>
Details for interface T	unnel0:		
Details for interface T Item Name	unnelO:	Item Value	
Details for interface T Item Name nterface	unnel0:	Item Value Tunnel0	
Details for interface T Item Name nterface PSec Profile	unnel0:	Item Value Tunnel0 CiscoCP_Profile1	
Details for interface T Item Name nterface PSec Profile P Address	unnel0:	Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2	
Details for interface T Item Name Interface PSec Profile P Address Description	unnelO:	Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 <none></none>	
Details for interface T Item Name Interface PSec Profile P Address Description Funnel Bandwidth	unnelO:	Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 <none> 1000</none>	
Details for interface T Item Name Interface PSec Profile P Address Description Funnel Bandwidth MTU	unnelO:	Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 «None» 1000 1400 DM/RNI NW/	
Details for interface T Item Name Interface IP Sec Profile IP Address Description Funnel Bandwidth VITU NHRP Authentication VIHRP Network ID	unnel0:	Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 <none> 1000 1400 DMVPN_NW 100000</none>	
Details for interface T Item Name Interface IPSec Profile IP Address Description Tunnel Bandwidth MTU NHRP Authentication NHRP Network ID NHRP Hold Time	unnelO:	Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 <none> 1000 1400 DMVPN_NW 100000 360</none>	

MTU 및 터널 키와 같은 터널 인터페이스 매개변수는 General 탭에서 수정됩니다.

eneral NHRP	Routing
IP address:	192.168.10.2
Mask:	255.255.255.0 24
- Tunnel Source:	2
Interface:	GigabitEthernet0/0
C IP address:	
Tunnel Destination	int GRE Turnel
Tunnel Destination This is an multipo P / Hostname:	int GRE Tunnel
Tunnel Destination This is an multipo This is an multipo The / Hostname: PSec Profile: MTU:	: int GRE Tunnel CiscoCP_Proti Add 1400
Tunnel Destination This is an multipo This is an multipo The flostname: PSec Profile: MTU: Bandwidth:	r: int GRE Tunnel CiscoCP_Protl M Add 1400 1000
Tunnel Destination This is an multipo This is an multipo The Profile: PSec Profile: MTU: Bandwidth: Delay:	: int GRE Tunnel CiscoCP_Proti Add 1400 1000 1000

1. NHRP 관련 매개변수는 NHRP 탭의 요구 사항에 따라 찾아 *수정됩니다*. 스포크 라우터의 경 우 NHS를 허브 라우터의 IP 주소로 볼 수 있어야 합니다. NHRP 매핑을 추가하려면 NHRP

DMVPN Tunnel Config	guration
General NHRP R	outing
Authentication String:	DMVPN_N/V
Hold Time:	360
Network ID:	100000
Next Hop Servers	
Next Hop Servers	Add
	Delete
NHRP Map	Mask
«None»	«None»
	> Decie
OK	Cancel Help

2. 네트워크 설정에 따라 NHRP 매핑 매개변수를 다음과 같이 구성할 수 있습니다

Statically configure t	the IP-to-NMBA address mapping
of IP destinations of	connected to a NBMA network.
Destination rea	chable through NBMA network
IP Address	
in Mudiroba.	
Mask (Optional):	19 I
NBMA address	directly reachable
IP Address.	
Configure NBMA ad	dresses used as destinations for broadc
or multicast packets	to be sent over a tunnel network.
Oynamically add	i spokes' IP addresses to hub's multicas
C IP address of N	AMA address directly reachable
· In address of N	

라우팅 관련 매개변수는 라우팅(Routing) 탭 아래에서 보고 *수정됩니다*.

Beneral NHRP Routin	a
Routing Protocol:	OSPF
Ø OSPF	
OSPF Network Type:	point-to-multipoint
OSPF Priority:	
Hello Interval:	-
Dead Interval:	

<u>추가 정보</u>

DMVPN 터널은 다음 두 가지 방법으로 구성됩니다.

- 허브를 통한 스포크 간 통신
- 허브가 없는 스포크 간 통신

이 문서에서는 첫 번째 방법만 설명합니다. 스포크 투 스포크(spoke-to-spoke) 동적 IPSec 터널을 설정하기 위해 이 접근 방식을 사용하여 DMVPN 클라우드에 스포크를 추가합니다.

- 1. DMVPN 마법사를 시작하고 Spoke 구성 옵션을 선택합니다.
- 2. DMVPN *Network Topology(DMVPN 네트워크 토폴로지*) 창에서 *Hub and Spoke 네트워크* 옵션 대신 *Full meshed network* 옵션을 선택합니다

DMVPN Spoke Wizard - 10% Complete



DMVPN Network Topology

Select the DMVPN network topology.

C Hub and Spoke network

In this topology, all DMVPN traffic is routed through the hub. A point-to-point GRE interface will be configured on the spoke, and the spoke will use it to create a tunnel to the hub which will remain up. Spokes do not create GRE tunnels to other spokes in this topology.

Fully meshed network

In this topology, the spoke dynamically establishes a direct tunnel to another spoke device, and sends DMVPN traffic directly to it. A multipoint GRE tunnel interface is configured on the spoke to support this functionality.

Note: Cisco supports fully meshed DMVPN networks only in the following Cisco IOS images: 12.3(8)T1 and 12.3(9) or later.



< Back Next > Finish Cancel Help

3. 이 문서의 다른 구성과 동일한 단계를 사용하여 나머지 구성을 완료합니다.

<u>다음을 확인합니다.</u>

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

<u>관련 정보</u>

- Cisco Dynamic Multipoint VPN: 간단하고 안전한 지사 간 커뮤니케이션
- IOS 12.2 DMVPN(Dynamic Multipoint VPN)
- <u>기술 지원 및 문서 Cisco Systems</u>

×