

FNS
 (Fundamental Network Security)
Ch12. IPsec VPN

/

[hjlee@dongseo.ac.kr](mailto:hjee@dongseo.ac.kr)
<http://kowon.dongseo.ac.kr/~hjlee>
<http://crypto.dongseo.ac.kr>

2005-11-14 http://kowon.dongseo.ac.kr/~hjlee 1

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 - 사이트 간 IPsec VPN 구축 실습

이번 강의의 학습목표를 살펴본도록 하겠습니다.

학습 목표

- VPN 기능 지원용 위한 컴퓨터 준비 작업을 할 수 있다.
- CA 지원 기능을 설정할 수 있다.
- IKE 파라미터를 설정할 수 있다.
- IPsec 파라미터를 설정할 수 있다.
- IPsec 구성을 검증하고 테스트할 수 있다.

2005-11-14 http://kowon.dongseo.ac.kr/~hjlee 2

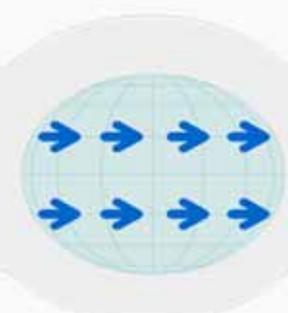
http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

12회차 : 사이트 간 IPSec VPN 구축 실습

강유 키를 이용한 IPSec 설정 실습

목표 ▶

- VPN 기능 지원용 위한 라우터 준비
- IKE (Internet Key Exchange) 파라미터 설정
- IPSec 파라미터 설정
- IKE/IPSec 설정 확인
- IPSec VPN 구성 검증 및 테스트



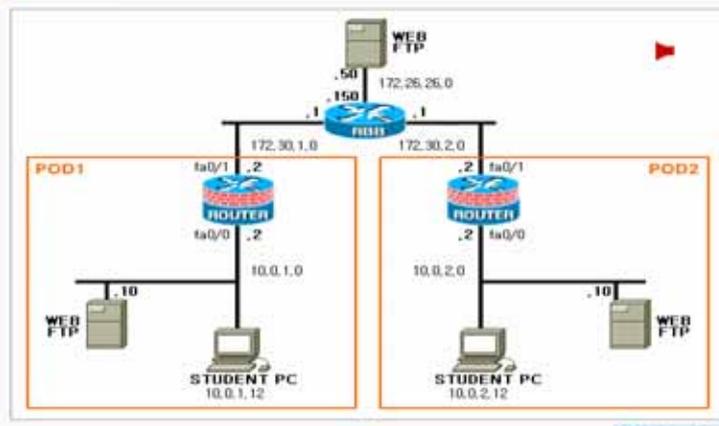
2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 3

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

12회차 : 사이트 간 IPSec VPN 구축 실습

강유 키를 이용한 IPSec 설정 실습

실습 도출로지



2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 4

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

12회차 : 사이트 간 IPSec VPN 구축 실습

강유 키를 이용한 IPSec 설정 실습

실습

제 1 단계: VPN 기능 지원용 라우터 준비

- IKE 및 IPSec 정책을 설정한다. 본 실험에서는 특별히 특별 값을 입력하도록 지시하지 않는 한 디폴트 값을 사용한다. 본 실험에서 사용하는 일반적인 보안 정책은 다음과 같다.
 - IKE 정책은 공유 키 (pre-shared key)를 사용하는 것이다.
 - IPSec 정책은 DES (Data Encryption Standard) 암호화를 이용한 ESP (Encapsulating Security Payload) 모드를 사용하는 것이다.
 - IPSec 정책은 경계 라우터 간의 모든 트래픽을 암호화하는 것이다.

Q 피어 (peer) 라우터 간의 연결성을 확인하고자 한다. POD 1 라우터에서 POD 2 라우터로의 연결성 확인을 위해서는 어떤 명령어를 입력해야 하는가? (*입력 후 Enter)

A Router1#ping 172.30.2.2

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 5

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

12회차 : 사이트 간 IPSec VPN 구축 실습

강유 키를 이용한 IPSec 설정 실습

실습

제 2 단계: IKE 파라미터 설정

Q Diffie-Hellman 그룹을 설정한다. (*입력 후 Enter)

A Router1(config-isakmp)#group 1

Q 해시 알고리즘을 'md5'로 설정한다. (*입력 후 Enter)

A Router1(config-isakmp)#hash md5

Q IKE SA (security association) lifetime를 86400으로 설정한다. (*입력 후 Enter)

A Router1(config-isakmp)#lifetime 86400

Q config-isakmp 모드를 빠져 나와 공유 키 (pre-shared key: netchannel)와 상대 주소 (peer address: 172.30.2.2)를 설정한다. (*입력 후 Enter)

A Router1(config-isakmp)#exit
Router1(config)#crypto isakmp key netchannel address 172.30.2.2

Q 설정한 crypto isakmp 정책을 확인한다. (*입력 후 Enter)

A Router1#show crypto isakmp policy

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 6

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

12회차 - 사이트 간 IPSec VPN 구축 실습

강유 키를 이용한 IPSec 설정 실습

실습

제 3 단계: IPSec 파라미터 설정

Q 아래의 파라미터를 이용하여 transform set을 정의한다.(×입력 후 Enter) **conf1**

- Transform set 이름: boan
- ESP 프로토콜: des
- 모드: tunnel

A Router(config)#crypto ipsec transform-set boan esp-des
Router(config-crypto-trans)#mode tunnel

Q Transform set 설정을 확인한다.(×입력 후 Enter)

A Router#show crypto ipsec transform-set boan

Q 아래의 파라미터를 이용하여 crypto access list를 설정한다.(×입력 후 Enter) **conf1**

- 허용할 트래픽: 모두
- 상대 주소: 상대 라우터의 외부 인터페이스
- ACL 번호: 102
- 프로토콜: 모든 인터넷 프로토콜

A Router(config)#access-list 102 permit ip host 172.30.1.2 host 172.30.2.2

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 7

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

12회차 - 사이트 간 IPSec VPN 구축 실습

강유 키를 이용한 IPSec 설정 실습

실습

제 3 단계: IPSec 파라미터 설정

Q 아래의 파라미터를 이용하여 crypto map을 설정한다.

- Map 이름: boanmap
- Map 번호: 10
- 키 교환 유형: isakmp
- 상대 (peer): 172.30.2.2
- Transform set 이름: boan
- ACL 매치 어드레스: 102

Q 우선, 사용할 map 이름, map 번호, 키 교환 유형을 설정한다.(×입력 후 Enter)

A Router(config)#crypto map boanmap 10 ipsec-isakmp

Q 현재의 map과 함께 사용할 ACL을 지정한다.(×입력 후 Enter)

A Router(config-crypto-map)#match address 102

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 8

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 9

The screenshot shows a web browser window with the URL `http://203.241.187.50:8080 - Network - Microsoft Internet Explorer`. The page title is "12회차 : 사이트 간 IPsec VPN 구축 실습" (12th Session: Site-to-Site IPsec VPN Construction Practice). The main content is under the heading "경유 키를 이용한 IPsec 설정 실습" (IPsec Configuration Practice Using a Relay Key). The current step is "제 3 단계: IPsec 파라미터 설정" (Step 3: IPsec Parameter Setting). The steps are as follows:

- Q** 앞에서 정의한 transform set을 지정한다.(×입력 후 Enter)
A Router1(config-crypto-map)#set transform-set boan
- Q** 호스트 이름 또는 IP 주소를 사용하여 VPN 상대 (peer)를 지정한다.(×입력 후 Enter)
A Router1(config-crypto-map)#set peer 172.30.2.2
- Q** 앞에서 작성한 crypto map을 인터페이스에 적용한다.(×입력 후 Enter)
A Router1(config)#interface FastEthernet 0/1
Router1(config-if)#crypto map boanmap

At the bottom of the browser window, there are buttons for "완료" (Done) and "인터넷" (Internet), and a page number "11/21".

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 10

The screenshot shows the same web browser window as above, but now at "제 4 단계: IPsec VPN 구성 검증 및 테스트" (Step 4: IPsec VPN Configuration Verification and Test). The steps are as follows:

- Q** IKE 정책을 확인한다.(×입력 후 Enter)
A Router1#show crypto isakmp policy
- Q** Transform set 설정을 확인한다.(×입력 후 Enter)
A Router1#show crypto ipsec transform-set boan
- Q** 설정된 crypto map을 확인한다.(×입력 후 Enter)
A Router1#show crypto map
- Q** isakmp SA와 ipsec SA를 확인한다.(×입력 후 Enter)
A Router1#show crypto isakmp sa
Router1#show crypto ipsec sa

At the bottom of the browser window, there are buttons for "메시지 보기" (View Message) and "실습하기" (Practice), and a page number "12/21".

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 11

12월 1차 사이버 보안 IPsec VPN 구축 실습

다지털 전환을 이용한 IPsec 설정 실습

목표

- IKE와 IPsec 설정을 위한 준비
- CA 지원 가능 설정
- IKE 설정
- IPsec 설정
- IPsec 구성 검증 및 테스트

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 12

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

12회차 - 사이트 간 IPSec VPN 구축 실습

다지털 인증을 이용한 IPSec 설정 실습

성수 토종모자

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 13

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

12회차 - 사이트 간 IPSec VPN 구축 실습

다지털 인증을 이용한 IPSec 설정 실습

성수

제 1 단계: IKE와 IPSec 설정 준비

- IKE 및 IPSec 정책을 골라준다. 본 실험에서는 특별히 특정 값을 입력하도록 지시하지 않는 한 디폴트 값을 사용한다. 본 실험에서 사용하는 보안 정책은 다음과 같다.
 - IKE 정책은 RSA signature 키를 사용하는 것이다.
 - IPSec 정책은 DES (Data Encryption Standard) 암호화를 이용한 ESP (Encapsulating Security Payload) 모드를 사용하는 것이다.
 - IPSec 정책은 관계 라우터 간의 모든 트래픽을 암호화하는 것이다.
- 라우터의 time zone, calendar, time 등을 설정한다. 라우터의 time zone 과 time 설정 명령어는 다음과 같다. **clock**

라우터의 time zone 설정 명령어	Router1(config)#clock timezone zone hours [minutes]
라우터의 time 설정 명령어	Router1#clock set hh:mm:ss day month year

- 실패 라우터와의 연결성을 'ping' 명령어로 확인한다.
- CA 서버 (172.26.26.50)와의 연결성을 'ping' 명령어로 확인한다.
- CA 서버로의 HTTP 세션 (<http://172.26.26.50/certsrv>)을 확인한다.

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 14

12회차 : 사이트 간 IPSec VPN 구축 실습

다지될 만큼을 이용한 IPSec 설정 실습

Q 제 2단계: CA 지원 기능 설정 **click**

Q 라우터의 도메인 이름 (netch.co.kr)을 설정한다.(×입력 후 Enter)

A Router1(config)#ip domain-name netch.co.kr

Q CA 서버의 할력 호스트 이름 (vpnc)과 IP 주소 (172.26.26.50) 설정을 정의한다.(×입력 후 Enter)

A Router1(config)#ip host vpnc 172.26.26.50

Q RSA usage-keys를 발생한다.(×입력 후 Enter) **click**

A Router1(config)#crypto key generate rsa usage-keys

Q CA 서버 trustpoint (서버 이름: vpnc) 설정 모드로 들어간다.(×입력 후 Enter)

A Router1(config)#crypto ca trustpoint vpnc

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 15

12회차 : 사이트 간 IPSec VPN 구축 실습

다지될 만큼을 이용한 IPSec 설정 실습

Q 제 2단계: CA 지원 기능 설정 **click**

Q Registration authority 모드를 선택한다.(×입력 후 Enter)

A Router1(ca-trustpoint)#enrollment mode ra

Q CA 서버의 URL (http://vpnc/certsrv/mscep/mscep.dll)을 지정한다.(×입력 후 Enter) **click**

A Router1(ca-trustpoint)#enrollment url http://vpnc/certsrv/mscep/mscep.dll

Q CRL (certificate revocation list)에의 접근이 불가능 경우에는, 상대편 (peer) 인증서를 수령할 수 있도록 라우터를 설정한다.(×입력 후 Enter)

A Router1(ca-trustpoint)#crl optional

Q PKI 디버깅 기능을 활성화한다.(×입력 후 Enter)

A Router1#debug crypto pki messages
Router1#debug crypto pki transactions

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 16

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

12회차 - 사이트 간 IPSec VPN 구축 실습

다지털 인증을 이용한 IPSec 설정 실습

실습

제 2 단계: CA 지원 기능 설정

Q CA 서버 인증을 수행하고 CA administrator와 CA 서버 fingerprint를 확인한다.
(<입력 후 Enter) **press**

A Router1(config)#crypto ca authenticate vpnca

Q CA 서버에 인증서를 등록한다.(<입력 후 Enter) **press**

A Router1(config)#crypto ca enroll vpnca

Q CA 인증서를 확인한다.(<입력 후 Enter)

A Router1#show crypto ca certificate

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 17

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

12회차 - 사이트 간 IPSec VPN 구축 실습

다지털 인증을 이용한 IPSec 설정 실습

실습

제 2 단계: CA 지원 기능 설정

Q CA 서버 인증을 수행하고 CA administrator와 CA 서버 fingerprint를 확인한다.
(<입력 후 Enter) **press**

A Router1(config)#crypto ca authenticate vpnca

Q CA 서버에 인증서를 등록한다.(<입력 후 Enter) **press**

A Router1(config)#crypto ca enroll vpnca

Q CA 인증서를 확인한다.(<입력 후 Enter)

A Router1#show crypto ca certificate

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 18

12회차 - 사이트 간 IPSec VPN 구축 실습

다지될 반복을 이용한 IPSec 설정 실습

3 단계: IKE 설정

Q: 라우터에 IKE/ISAKMP 기능을 활성화하기 위한 명령어를 입력한다. (×입력 후 Enter) **click**

A: Router(config)#crypto isakmp enable

Q: RSA signature를 사용한 IKE 정책을 생성한다. 이를 위해 우선 policy priority를 설정 (예: 110)하여 config-isakmp 모드로 들어간다. (×입력 후 Enter)

A: Router(config)#crypto isakmp policy 110

Q: RSA signature 인증을 하도록 설정한다. (×입력 후 Enter)

A: Router(config-isakmp)#authentication rsa-sig

Q: IKE 암호화를 'des'로 설정한다. (×입력 후 Enter) **click**

A: Router(config-isakmp)#encryption des

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 19

12회차 - 사이트 간 IPSec VPN 구축 실습

다지될 반복을 이용한 IPSec 설정 실습

3 단계: IKE 설정

Q: Diffie-Hellman 그룹을 설정한다. (×입력 후 Enter) **click**

A: Router(config-isakmp)#group 1

Q: 해시 알고리즘을 'md5'로 설정한다. (×입력 후 Enter)

A: Router(config-isakmp)#hash md5

Q: IKE SA (security association) lifetime를 86400으로 설정한다. (×입력 후 Enter)

A: Router(config-isakmp)#lifetime 86400

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 20

12회차 : 사이트 간 IPSec VPN 구축 실습

다지털 민중을 이용한 IPSec 설정 실습

실습

제 4 단계: IPSec 설정

이래의 파라미터를 이용하여 transform set을 정의한다.(×입력 후 Enter) **check**

- Transform set 이름: boan
- ESP 프로토콜: des
- 모드: tunnel

A Router1(config)#crypto ipsec transform-set boan esp-des
Router1(cfg-crypto-trans)#mode tunnel

Transform set 설정을 확인한다.(×입력 후 Enter)

A Router1#show crypto ipsec transform-set boan

이래 파라미터를 이용하여 crypto access list를 설정한다.(×입력 후 Enter) **check**

- 허용할 트래픽: 모두
- 상대 주소: 상대 라우터의 외부 인터페이스
- ACL 번호: 102
- 프로토콜: 모든 인터넷 프로토콜

A Router1(config)#access-list 102 permit ip host 172.30.1.2 host 172.30.2.2

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 21

12회차 : 사이트 간 IPSec VPN 구축 실습

다지털 민중을 이용한 IPSec 설정 실습

실습

제 4 단계: IPSec 설정

이래의 파라미터를 이용하여 crypto map을 설정한다,

- Map 이름: boanmap
- Map 번호: 10
- 키 교환 유형: isakmp
- 상대 (peer): 172.30.2.2
- Transform set 이름: boan
- ACL 매치 어드레스: 102

Q 우선, 사용할 map 이름, map 번호, 키 교환 유형을 설정한다.(×입력 후 Enter)

A Router1(config)#crypto map boanmap 10 ipsec-isakmp

Q 현재의 map과 함께 사용할 ACL을 지정한다.(×입력 후 Enter)

A Router1(config-crypto-map)#match address 102

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 22

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 23

The screenshot shows a web browser window titled "12회차: 사이트 간 IPsec VPN 구축 실습". The main heading is "다지형 인텔을 이용한 IPsec 설정 실습". Under the "실습" section, the current step is "제 4 단계: IPsec 설정".

Three Q/A pairs are listed:

- Q** 앞에서 정의한 transform set을 지정한다.(×입력 후 Enter)
A Router(config-crypto-map)#set transform-set boan
- Q** 호스트 이름 또는 IP 주소를 사용하여 VPN 상대 (peer)를 지정한다.(×입력 후 Enter)
A Router(config-crypto-map)#set peer 172.30.2.2
- Q** 앞에서 작성한 crypto map을 인터페이스에 적용한다.(×입력 후 Enter)
A Router(config)#interface FastEthernet 0/1
Router(config-if)#crypto map boanmap

At the bottom of the browser window, there are buttons for "완료" (Done) and "인터넷" (Internet).

2005-11-14 <http://kowon.dongseo.ac.kr/~hjlee> 24

The screenshot shows the same web browser window, but the current step is "제 5 단계: IPsec 구성 검증 및 테스트".

Four Q/A pairs are listed:

- Q** IKE 정책을 확인한다.(×입력 후 Enter)
A Router#show crypto isakmp policy
- Q** Transform set 설정을 확인한다.(×입력 후 Enter)
A Router#show crypto ipsec transform-set boan
- Q** 설정된 crypto map을 확인한다.(×입력 후 Enter)
A Router#show crypto map
- Q** Isakmp SA와 Ipsec SA를 확인한다.(×입력 후 Enter)
A Router#show crypto isakmp sa
Router#show crypto ipsec sa

At the bottom of the browser window, there are buttons for "메시지 보기" (View Message) and "실습하기" (Practice).

http://203.241.107.50:8080 - Unfiled Document - Microsoft Internet Explorer

공유 키를 이용한 IPSec 설정 실습

1. 컴퓨터 도메인 이름 설정 (neth.co.kr)
2. CA 서버의 호스트 이름 (opca)과 IP 주소 (172.26.26.50) 기록 잡기
3. RSA usage-key 발급
4. CA 서버 hostpoint 설정 모드 진입 (서버 이름: opca)
5. registration authority 정보 입력 (http://opca/cenury/maccsp/maccsp.dll)
6. CA 서버 IP를 지정
7. CSR 발급 불가 시 최대 인증서 수를 1로 설정
8. CA 서버 인증
9. CA 서버에 인증서 등록
10. CA 인증서 확인

공유 키를 이용한 IPSec 설정 실습

1. Router1(config)#ip domain-name neth.co.kr
2. Router1(config)#ip host opca 172.26.26.50
3. Router1(config)#crypto key generate rsa usage-keys
4. Router1(config)#crypto ca trustpoint opca
5. Router1(ca-trustpoint)#activation mode iv
6. Router1(ca-trustpoint)#activation url http://opca/cenury/maccsp/maccsp.dll
7. Router1(ca-trustpoint)#cert optional
8. Router1(ca-trustpoint)#end
9. Router1#show ipsec tunnel

2005-11-14 http://kowon.dongseo.ac.kr/~hjlee 25

http://203.241.107.50:8080 - Network - Microsoft Internet Explorer

12회차: 사이트 간 IPSec VPN 구축 실습

지금까지 공부한 내용을 요약하여 다시 한번 정리를 하도록 하겠습니다. 부족한 부분은 다시 한번 확인 하시기 바랍니다.

공유 키를 이용한 IPSec 설정 실습

암호의 두 지점 간을 인터넷을 통해 사이트 간 가상 사설망을 구축함으로써 안전한 데이터 통신을 할 수 있다. 사이트 간 상호 인증을 위하여 두 대의 라우터 사이에서 공유 키를 사용하고 IPSec 설정을 함으로써 secure VPN 게이트웨이를 구성할 수 있다. 설정 작업은 아래의 세 단계를 통하여 수행한다.

- 제 1 단계: VPN 지원 기능 준비
- 제 2 단계: 부드 파라미터 설정
- 제 3 단계: IPSec 파라미터 설정

디지털 인증을 이용한 IPSec 설정 실습

암호의 두 지점 간을 CA 서버를 사용하여 사이트 간 가상 사설망을 구축함으로써 안전한 데이터 통신을 할 수 있다. 이와 같이 구성된 가상 사설망을 디지털 인증을 이용한 IPSec VPN이라 하며, 이에 대한 설정 작업은 아래와 같은 네 단계를 통하여 수행한다.

- 제 1 단계: IKE/ISAKMP 설정 준비
- 제 2 단계: CA 지원 기능 설정
- 제 3 단계: 부드 설정
- 제 4 단계: IPSec 설정

완료

2005-11-14 http://kowon.dongseo.ac.kr/~hjlee 26

End of Lecture



2005-11-14

<http://kowon.dongseo.ac.kr/~hjlee>

27