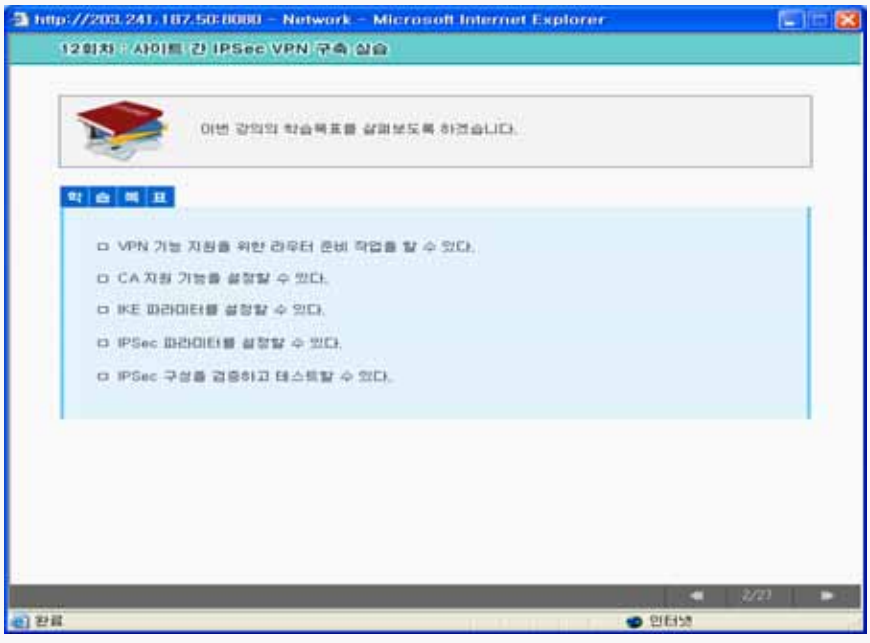
FNS

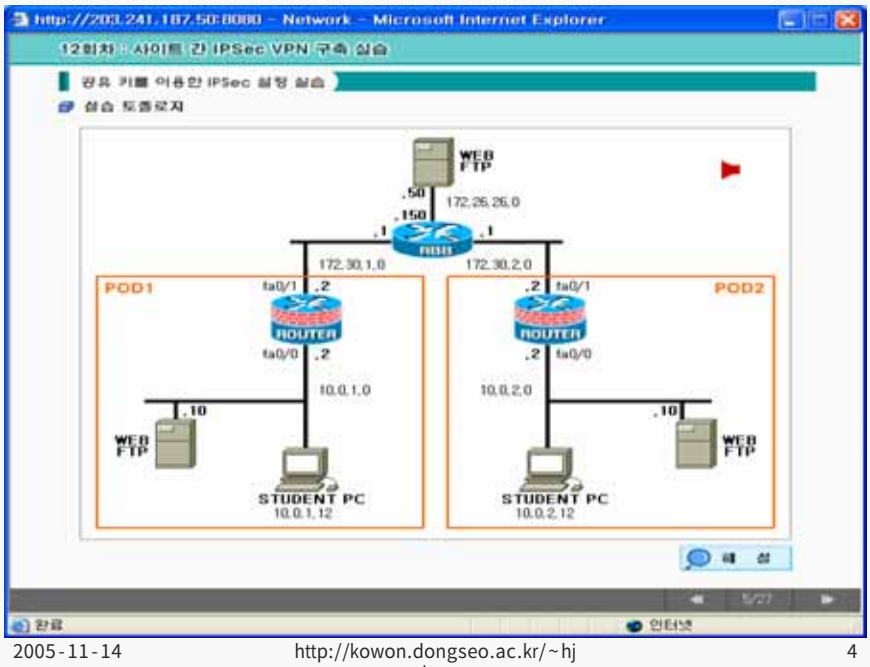
(Fundamental Network Security)

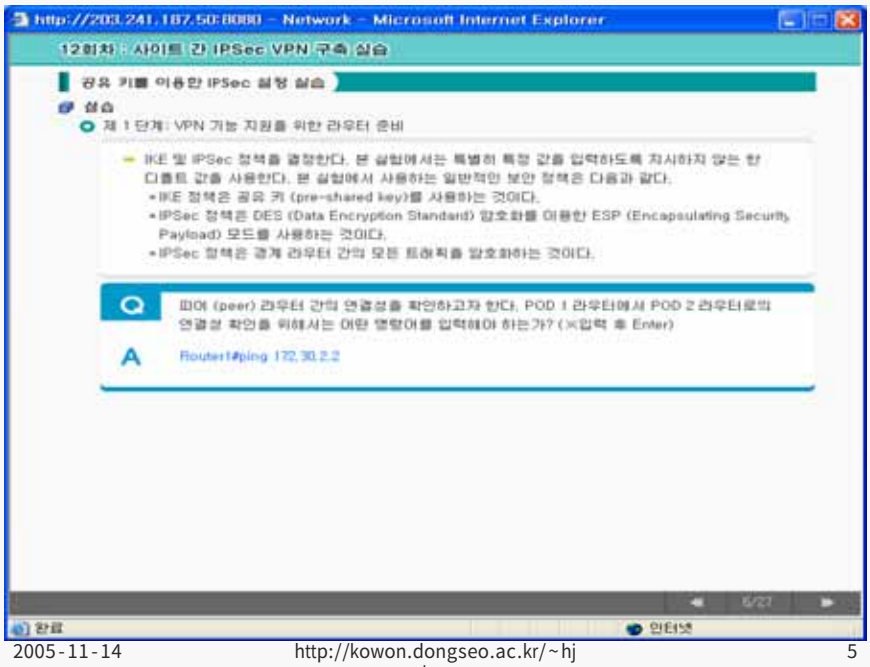
Ch12. 사이트간 IPSec VPN 구축 실습

동서대학교/인터넷공학부
이 훈 재
hjlee@dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee
http://crypto.dongseo.ac.kr



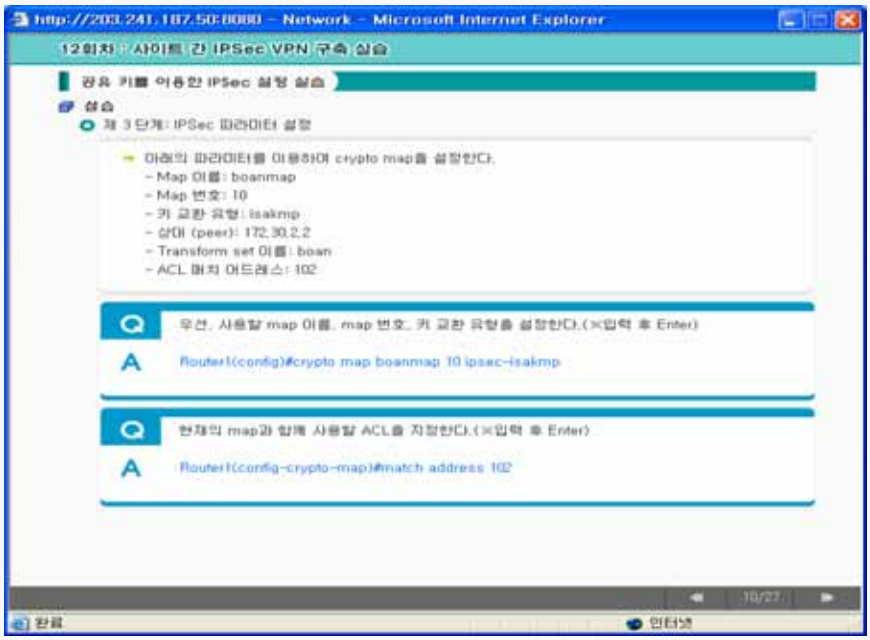

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
공유 키를 이용한 IPSec 설정 실습
목 표
VPN 기능 지원을 위한 라우터 준비
IKE (Internet Key Exchange) 파라미터 설정
IPSec 파라미터 설정
IKE/IPSec 설정 확인
IPSec VPN 구성 검증 및 테스트
3/27
완료
인터넷

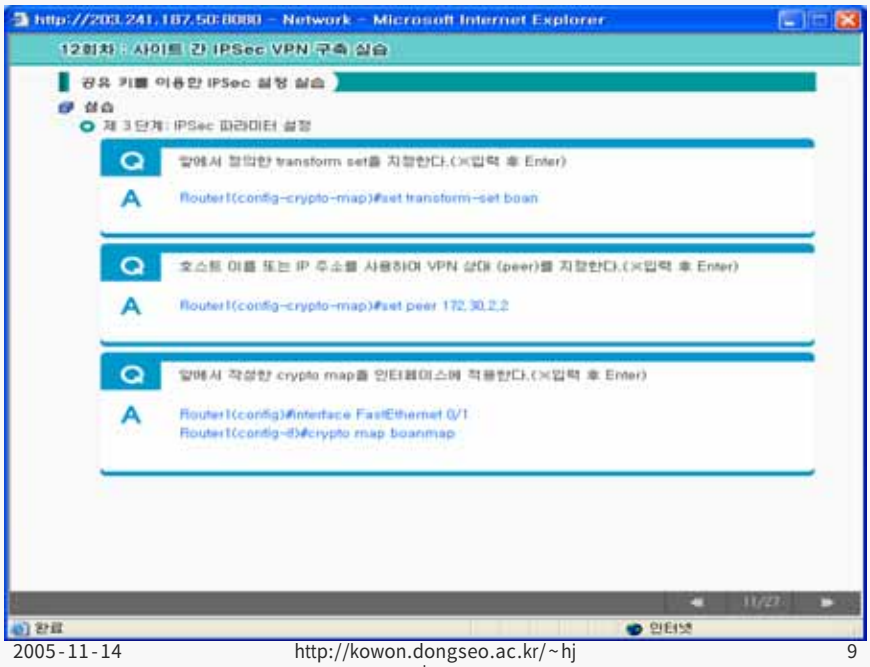

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
공유 키를 이용한 IPSec 설정 실습
실습 토폴로지
WEB FTP
.50
172.26.26.0
.150
.1
.1
ROUTER
172.30.1.0
172.30.2.0
POD1
POD2
fa0/1
.2
fa0/0
.2
ROUTER
10.0.1.0
10.0.2.0
.10
WEB FTP
STUDENT PC
10.0.1.12
STUDENT PC
10.0.2.12
해 설
5/27
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
공유 키를 이용한 IPSec 설정 실습
실습
제 1 단계: VPN 기능 지원을 위한 라우터 준비
IKE 및 IPSec 정책을 결정한다. 본 실습에서는 특별히 특정 값을 입력하도록 지시하지 않는 한 디폴트 값을 사용한다. 본 실습에서 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
5/27
완료
인터넷

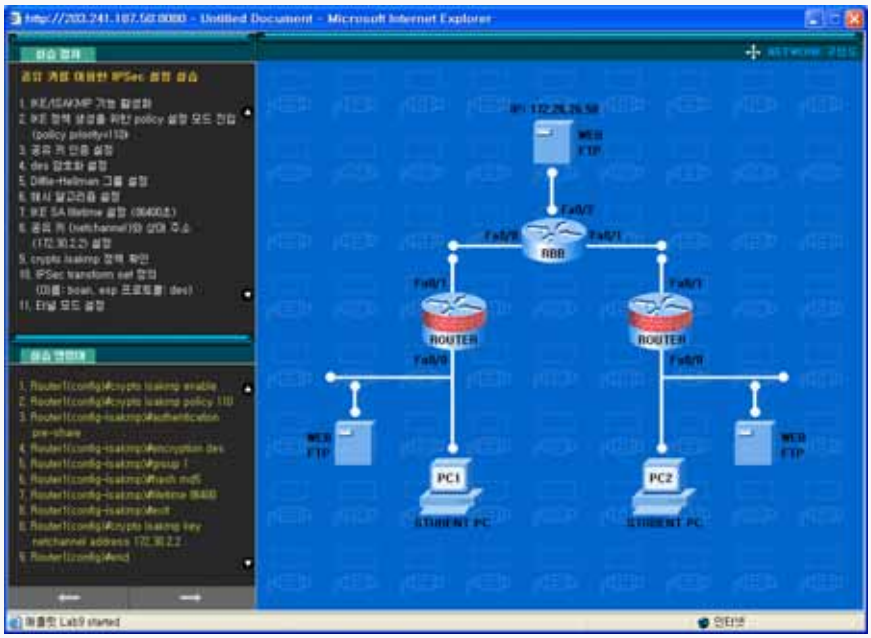

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
공유 키를 이용한 IPSec 설정 실습
실습
제 2 단계: IKE 파라미터 설정
Q
Diffie-Hellman 그룹을 설정한다.(↵입력 후 Enter)
A
Router1(config-isakmp)#group 1
Q
해시 알고리즘을 'md5'로 설정한다.(↵입력 후 Enter)
A
Router1(config-isakmp)#hash md5
Q
IKE SA (security association) lifetime을 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
5/27
완료
인터넷

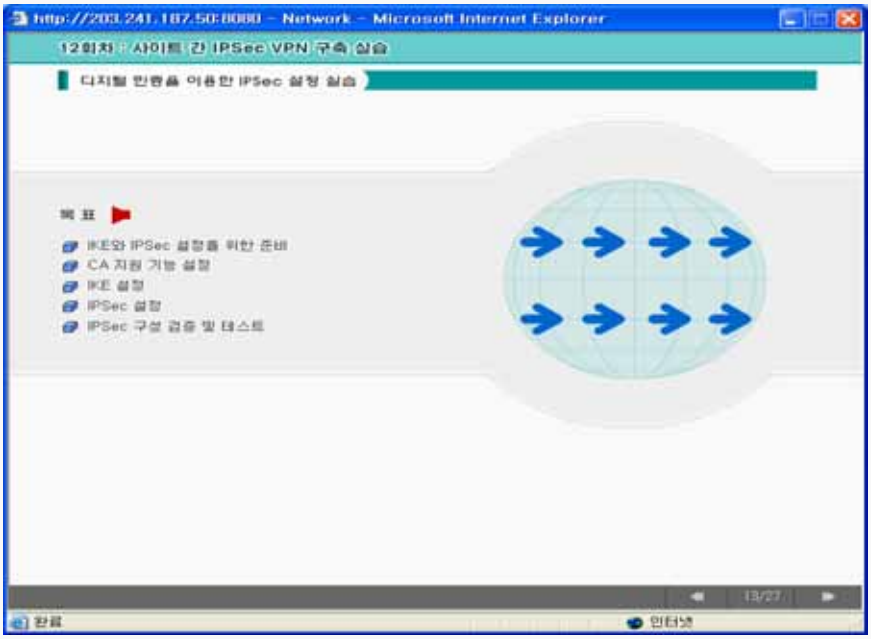

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
공유 키를 이용한 IPSec 설정 실습
실습
제 3 단계: IPSec 파라미터 설정
이래의 파라미터를 이용하여 transform set를 정의한다.(↵입력 후 Enter) click
- Transform set 이름: boan
- ESP 프로토콜: des
- 모드: tunnel
Router1(config)#crypto ipsec transform-set boan esp-des
Router1(cfg-crypto-trans)#mode tunnel
Transform set 설정을 확인한다.(↵입력 후 Enter)
Router1#show crypto ipsec transform-set boan
이래 파라미터를 이용하여 crypto access list를 설정한다.(↵입력 후 Enter) click
- 허용할 트래픽: 모두
- 상대 주소: 상대 라우터의 외부 인터페이스
- ACL 번호: 102
- 프로토콜: 모든 인터넷 프로토콜
Router1(config)#access-list 102 permit ip host 172.30.1.2 host 172.30.2.2
9/27
완료
인터넷

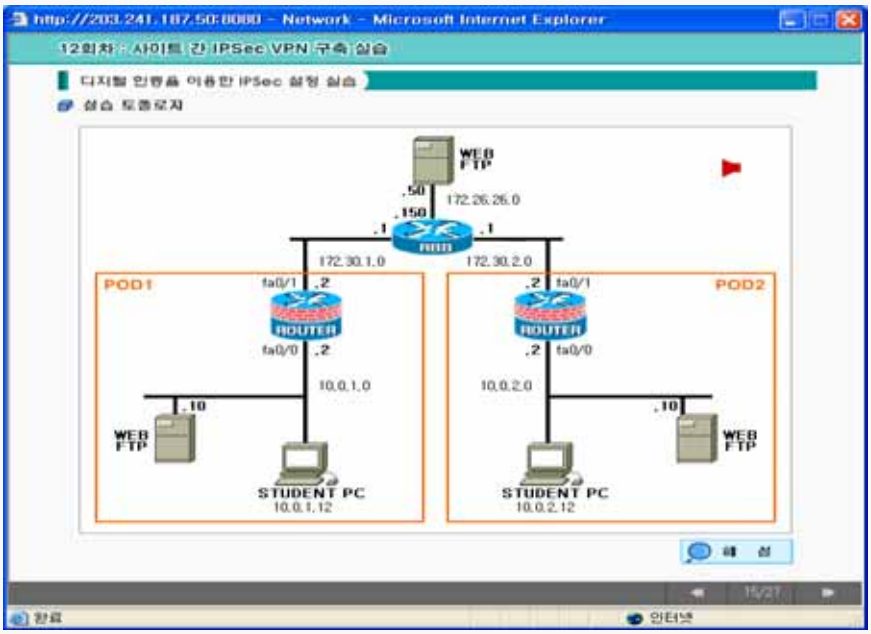

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
공유 키를 이용한 IPSec 설정 실습
실습
제 3 단계: IPSec 파라미터 설정
이래의 파라미터를 이용하여 crypto map를 설정한다.
- Map 이름: boanmap
- Map 번호: 10
- 키 교환 유형: isakmp
- 상대 (peer): 172.30.2.2
- Transform set 이름: boan
- ACL 매치 어드레스: 102
우선, 사용할 map 이름, map 번호, 키 교환 유형을 설정한다.(↵입력 후 Enter)
Router1(config)#crypto map boanmap 10 ipsec-isakmp
현재의 map과 함께 사용할 ACL을 지정한다.(↵입력 후 Enter)
Router1(config-crypto-map)#match address 102
10/27
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
공유 키를 이용한 IPSec 설정 실습
실습
제 3 단계: IPSec 파라미터 설정
앞에서 정의한 transform set을 지정한다.(※입력 후 Enter)
Router1(config-crypto-map)#set transform-set boan
호스트 이름 또는 IP 주소를 사용하여 VPN 상대 (peer)를 지정한다.(※입력 후 Enter)
Router1(config-crypto-map)#set peer 172.30.2.2
앞에서 작성한 crypto map을 인터페이스에 적용한다.(※입력 후 Enter)
Router1(config)#interface FastEthernet 0/1
Router1(config-if)#crypto map boanmap
11/27
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
공유 키를 이용한 IPSec 설정 실습
실습
제 4 단계: IPSec VPN 구성 검증 및 테스트
IKE 정책을 확인한다.(※입력 후 Enter)
Router1#show crypto isakmp policy
Transform set 설정을 확인한다.(※입력 후 Enter)
Router1#show crypto ipsec transform-set boan
설정된 crypto map을 확인한다.(※입력 후 Enter)
Router1#show crypto map
isakmp SA와 ipsec SA를 확인한다.(※입력 후 Enter)
Router1#show crypto isakmp sa
Router1#show crypto ipsec sa
여기서 끝!!
실습하기
12/27
완료
인터넷


ROUTER
ROUTER
PC1
PC2


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
목 표
IKE와 IPSec 설정을 위한 준비
CA 지원 기능 설정
IKE 설정
IPSec 설정
IPSec 구성 검증 및 테스트


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
실습 토폴로지
WEB FTP
.50
.150
172.26.26.0
.1
.1
172.30.1.0
172.30.2.0
POD1
POD2
fa0/1
.2
ROUTER
fa0/0
.2
10.0.1.0
10.0.2.0
.10
WEB FTP
STUDENT PC
10.0.1.12
STUDENT PC
10.0.2.12
15/27
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
실습
제 1 단계: IKE와 IPSec 설정 준비
IKE 및 IPSec 정책을 결정한다. 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 공개 라우터 간의 모든 트래픽을 암호화하는 것이다.
라우터의 time zone, calendar, time 등을 설정한다. 라우터의 time zone 과 time 설정 명령어는 다음과 같다. click
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
상대 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.
16/27
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
실습
제 2 단계: CA 지원 기능 설정
click
라우터의 도메인 이름 (netch.co.kr)을 설정한다.(↵입력 후 Enter)
Router1(config)#ip domain-name netch.co.kr
CA 서버의 정적 호스트 이름 (vpnca)과 IP 주소 (172.26.26.50: super server)
맵핑을 정의한다.(↵입력 후 Enter)
Router1(config)#ip host vpnca 172.26.26.50
RSA usage-keys를 발생한다.(↵입력 후 Enter)
click
Router1(config)#crypto key generate rsa usage-keys
CA 서버 trustpoint (서버 이름: vpnca) 설정 모드로 들어간다.(↵입력 후 Enter)
Router1(config)#crypto ca trustpoint vpnca
17/27
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
실습
제 2 단계: CA 지원 기능 설정
Registration authority 모드를 선택한다.(↵입력 후 Enter)
Router1(ca-trustpoint)#enrollment mode ra
CA 서버의 URL (http://vpnca/certsrv/mscep/mscep.dll)을 지정한다.(↵입력 후 Enter)
click
Router1(ca-trustpoint)#enrollment url http://vpnca/certsrv/mscep/mscep.dll
CRL (certificate revocation list)에의 접근이 불가할 경우에는, 상대편 (peer) 인증서를
수용할 수 있도록 라우터를 설정한다.(↵입력 후 Enter)
Router1(ca-trustpoint)#crl optional
PKI 디버깅 기능을 활성화한다.(↵입력 후 Enter)
Router1#debug crypto pki messages
Router1#debug crypto pki transactions
18/27
완료
인터넷

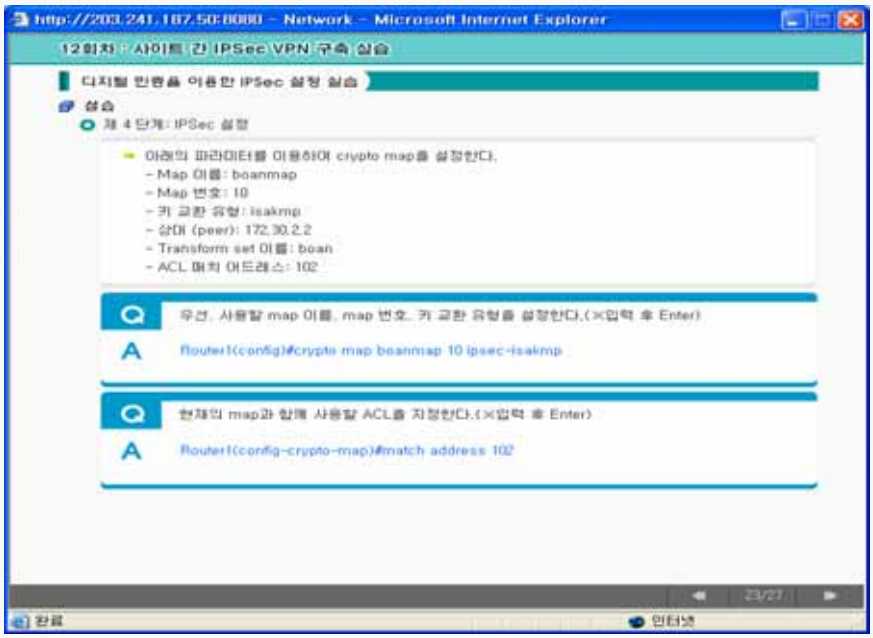

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
실습
제 2 단계: CA 지원 기능 설정
CA 서버 인증을 수행하고 CA administrator와 CA 서버 fingerprint를 확인한다.
(※입력 후 Enter) CHECK
Router1(config)#crypto ca authenticate vpnca
CA 서버에 인증서를 등록한다.(※입력 후 Enter) CHECK
Router1(config)#crypto ca enroll vpnca
CA 인증서를 확인한다.(※입력 후 Enter)
Router1#show crypto ca certificate
19/27
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
실습
제 2 단계: CA 지원 기능 설정
CA 서버 인증을 수행하고 CA administrator와 CA 서버 fingerprint를 확인한다.
(※입력 후 Enter) CHECK
Router1(config)#crypto ca authenticate vpnca
CA 서버에 인증서를 등록한다.(※입력 후 Enter) CHECK
Router1(config)#crypto ca enroll vpnca
CA 인증서를 확인한다.(※입력 후 Enter)
Router1#show crypto ca certificate
19/27
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
실습
제 3 단계: IKE 설정
라우터에 IKE/ISAKMP 기능을 활성화하기 위한 명령어를 입력한다.(↵입력 후 Enter) click
Router1(config)#crypto isakmp enable
RSA signature를 사용한 IKE 정책을 생성한다. 이를 위해 우선 policy priority를 설정
(예: 110)하여 config-isakmp 모드로 들어간다.(↵입력 후 Enter)
Router1(config)#crypto isakmp policy 110
RSA signature 인증을 하도록 설정한다.(↵입력 후 Enter)
Router1(config-isakmp)#authentication rsa-sig
IKE 암호화를 'des'로 설정한다.(↵입력 후 Enter) click
Router1(config-isakmp)#encryption des
20/27
완료
인터넷

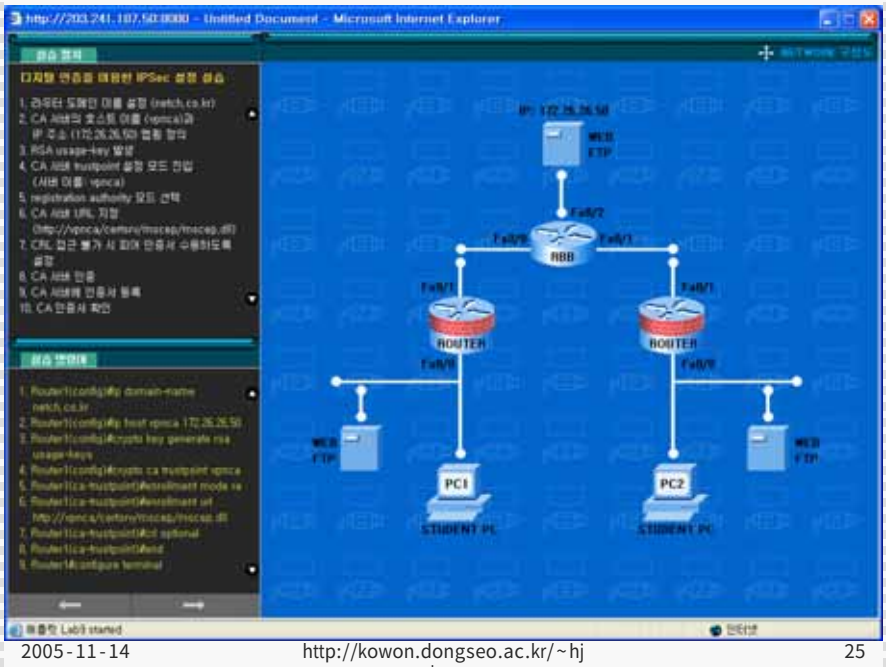

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
실습
제 3 단계: IKE 설정
Diffie-Hellman 그룹을 설정한다.(↵입력 후 Enter) click
Router1(config-isakmp)#group 1
해시 알고리즘을 'md5'로 설정한다.(↵입력 후 Enter)
Router1(config-isakmp)#hash md5
IKE SA (security association) lifetime을 86400으로 설정한다.(↵입력 후 Enter)
Router1(config-isakmp)#lifetime 86400
21/27
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
실습
제 4 단계: IPSec 설정
Click
- Transform set 이름: boan
- ESP 프로토콜: des
- 모드: tunnel
Router1(config)#crypto ipsec transform-set boan esp-des
Router1(cfg-crypto-trans)#mode tunnel
Router1#show crypto ipsec transform-set boan
Click
- 허용할 트래픽: 모두
- 상대 주소: 상대 라우터의 외부 인터페이스
- ACL 번호: 102
- 프로토콜: 모든 인터넷 프로토콜
Router1(config)#access-list 102 permit ip host 172.30.1.2 host 172.30.2.2
22/27
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
실습
제 4 단계: IPSec 설정
- Map 이름: boanmap
- Map 번호: 10
- 키 교환 유형: isakmp
- 상대 (peer): 172.30.2.2
- Transform set 이름: boan
- ACL 매치 어드레스: 102
Router1(config)#crypto map boanmap 10 ipsec-isakmp
Router1(config-crypto-map)#match address 102
23/27
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
실습
제 4 단계: IPSec 설정
앞에서 정의한 transform set을 지정한다.(※입력 후 Enter)
Router1(config-crypto-map)#set transform-set boan
호스트 이름 또는 IP 주소를 사용하여 VPN 상대 (peer)를 지정한다.(※입력 후 Enter)
Router1(config-crypto-map)#set peer 172.30.2.2
앞에서 작성한 crypto map을 인터페이스에 적용한다.(※입력 후 Enter)
Router1(config)#interface FastEthernet 0/1
Router1(config-if)#crypto map boanmap
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
12회차 : 사이트 간 IPSec VPN 구축 실습
디지털 인증을 이용한 IPSec 설정 실습
실습
제 5 단계: IPSec 구성 검증 및 테스트
IKE 정책을 확인한다.(※입력 후 Enter)
Router1#show crypto isakmp policy
Transform set 설정을 확인한다.(※입력 후 Enter)
Router1#show crypto ipsec transform-set boan
설정된 crypto map을 확인한다.(※입력 후 Enter)
Router1#show crypto map
isakmp SA와 ipsec SA를 확인한다.(※입력 후 Enter)
Router1#show crypto isakmp sa
Router1#show crypto ipsec sa
여기서 잠깐!
실습하기
완료
인터넷


http://203.241.107.50:8080 - Untitled Document - Microsoft Internet Explorer
디지털 인증을 이용한 IPSec 설정 실습
ABB
ROUTER
ROUTER
PC1
PC2
STUDENT PC
STUDENT PC


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
임의의 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 : IKE 파라미터 설정
제 3 단계 : IPSec 파라미터 설정
디지털 인증을 이용한 IPSec 설정 실습
임의의 두 지점 간을 CA 서버를 사용하여 사이트 간 가상 사설망을 구축함으로써 안전한 데이터 통신을
할 수도 있다. 이와 같이 구성한 가상 사설망을 디지털 인증을 이용한 IPSec VPN이라 하며, 이에 대한
설정 작업은 아래와 같은 네 단계를 통하여 수행한다.
제 1 단계 : IKE/IPSec 설정 준비
제 2 단계 : CA 지원 기능 설정
제 3 단계 : IKE 설정
제 4 단계 : IPSec 설정
완료
인터넷

End of Lecture