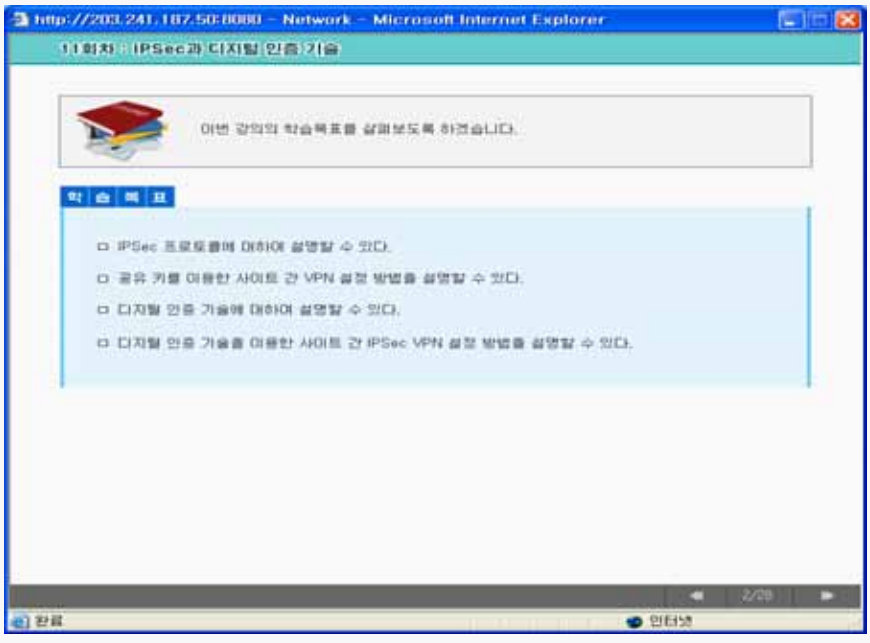
FNS

(Fundamental Network Security)

Ch11. IPSec (IP Security)과 디지털 서명 기술

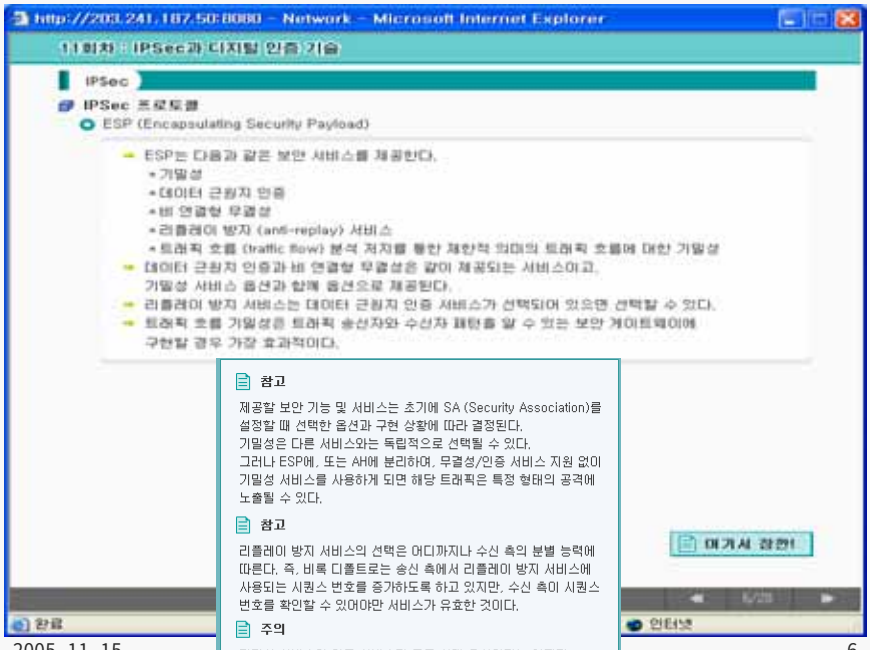
동서대학교/인터넷공학부
이 훈 재
hjlee@dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee
http://crypto.dongseo.ac.kr

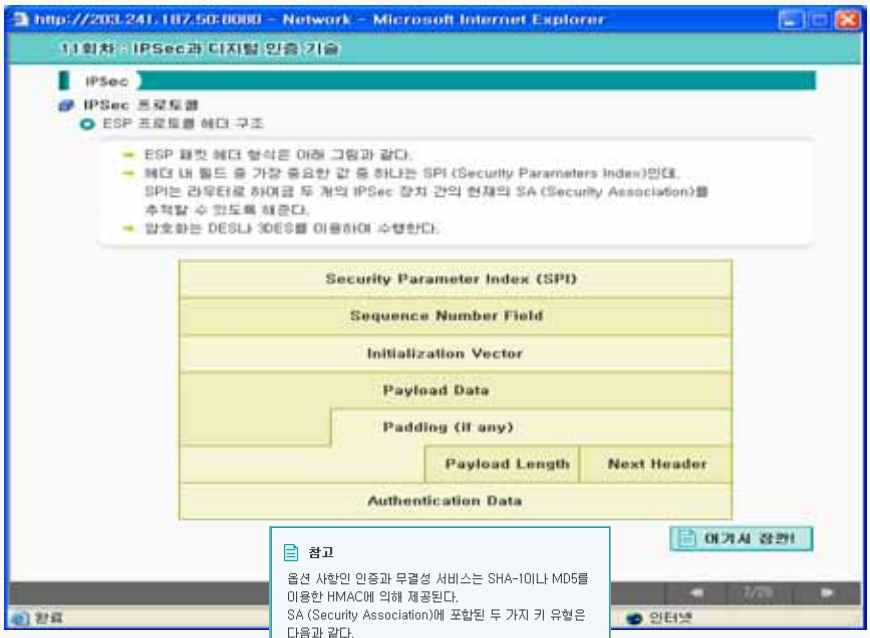



http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
IPSec 개요
IPSec이란?
IPSec은 데이터를 보호하기 위해 네트워크 계층에서 사용하는 보안 프로토콜 및 알고리즘으로서, IP 패킷을 보호하고 인증한다.
개방형 표준 체제로서 알고리즘에 독립적이다.
데이터 기밀성은 물론 데이터 무결성, 그리고 데이터 근원지 인증 기능 등을 제공한다.
IPSec을 구성하는 두 가지 프로토콜
ESP (Encapsulating Security Payload)
* 패킷 데이터에 대한 캡슐화 과정을 수행하여 보안성을 지원하지만, 패킷 헤더 보호 기능은 없다.
* 즉, ESP는 데이터 기밀성을 위하여 페이로드 (payload)에 대한 암호화를 수행한다.
AH (Authentication Header)
* AH 프로토콜은 데이터는 물론 헤더도 포함하여 전체 IP 데이터그램을 보호한다.
* AH는 IP 데이터그램에 대한 무결성 확인 기능을 수행한다.
IP Header
AH Header
ESP Header
IP Data
참고
ESP와 AH는 비록 공개 키 알고리즘도 사용할 수는 있지만 일반적으로 대칭 비밀 키 알고리즘을 사용한다.
여기서 잠깐!
완료
인터넷

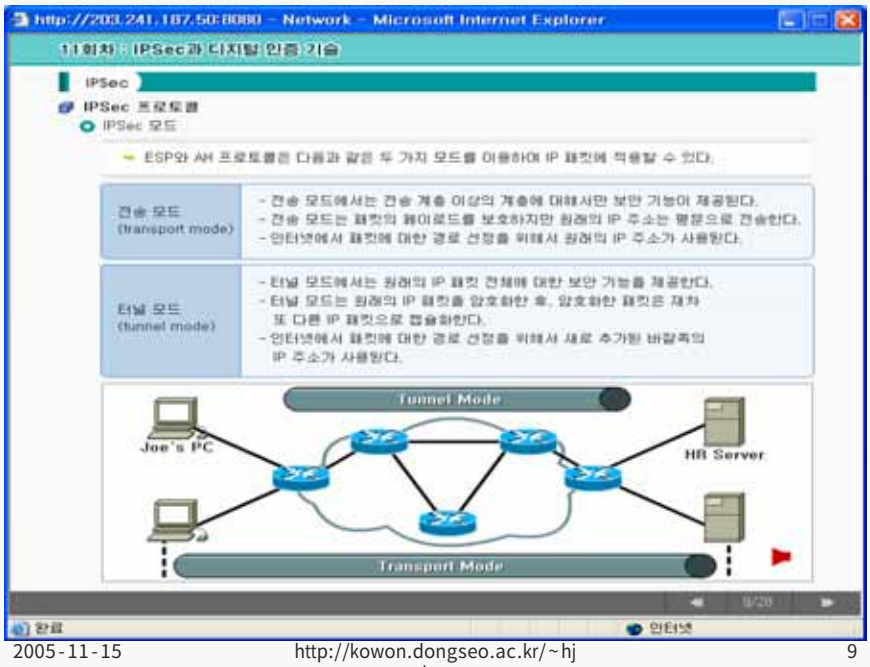

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
IPSec 프로토콜
AH (Authentication Header)
AH 프로토콜은 데이터 패킷의 근원지 인증, IP 데이터그램에 대한 무결성 확인, 시퀀스 번호를 이용한 리플레이 (replay) 탐지 및 보호 기능을 제공한다.
그러나, 기밀성이나 암호화 기능을 제공되지 않는다.
아래 그림은 IPSec에서 AH가 어떻게 생성되는지를 보여준다.
Original IP Datagram
IP Header
Other Headers and Payload
Secret Key
HMAC Algorithim (such as keyed SHA-1)
IP Header
AH
Other Headers and Payloads
Authenticated IP Datagram
여기서 잠깐!
AH (Authentication Header)
AH는 상위 계층 프로토콜 데이터뿐만 아니라 IP 헤더에 대한 인증 기능도 제공하지만, IP 헤더의 일부는 전송 도중 변경될 수 있다. 송신 측에서는 이와 같은 필드가 수신 측에 도착했을 때 어떻게 변경되는지 예측할 수 없다.
따라서 이러한 필드 내의 값은 AH 프로토콜에 의해 보호될 수 없다.
완료
인터넷

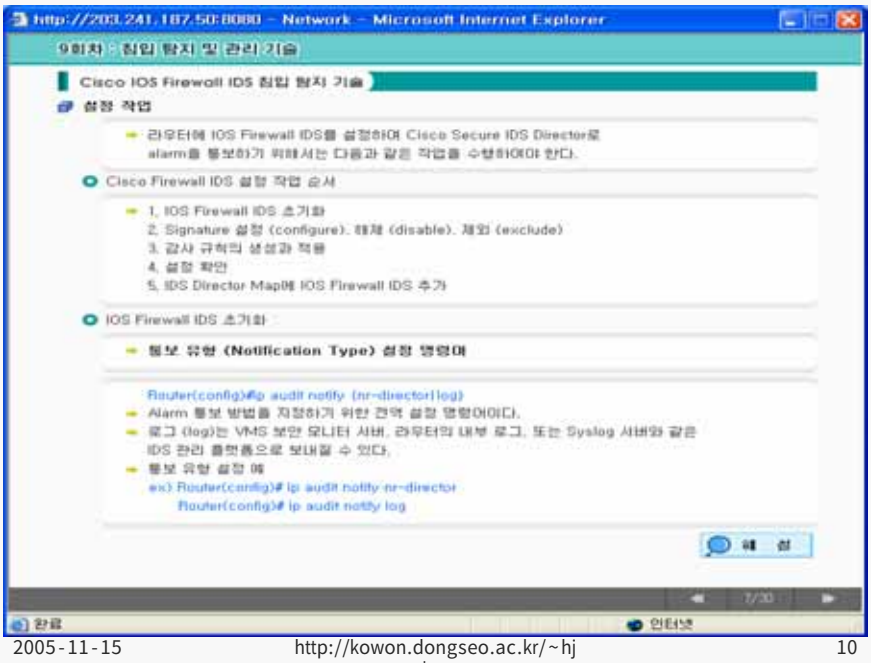

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
IPSec 프로토콜
AH 프로토콜 헤더 구조
32 비트의 SPI (Security Parameter Index) 값은 해당 패킷에 대하여 사용된 보안 연계 (SA: Security Association) 정보를 나타낸다.
64 비트의 시퀀스 번호 (Sequence Number)는 패킷 리플레이를 방지한다.
인증 데이터 (Authentication Data) 필드는 해당 패킷에 대한 HMAC 값이다.
Next Header
Payload Length
RESERVED
Security Parameter Index (SPI)
Sequence Number
Authentication Data
여기서 잠깐!
ESP가 모든 보안 서비스 기능을 제공하는 것 같은데도 AH를 사용하는 이유는 무엇일까?
- AH는 ESP보다 오버헤드가 적다.
- AH 기술에 대해서는 수출 규제가 없다.
- AH는 IPv6 호환성을 위한 강제 사항이다.
Spi
송신지 또는 수신지 IP주소와 Ipsec 프로토콜등과 함께 데이터그램이 속하는 트래픽을 위한 보안 연계(sa)를 고유하게 식별하기 위해서 사용된다.
Sequenvce number
일정하게 증가하는 카운트 값으로서 sa가 설정될때 0으로 초기화 된다. 패킷의 재전송을 방지 하기위해 사용되며 패킷 재전송은 침입자가 데이터그램을 가로채 두었다가 다시 전송하는것을 가리킨다.
완료
인터넷

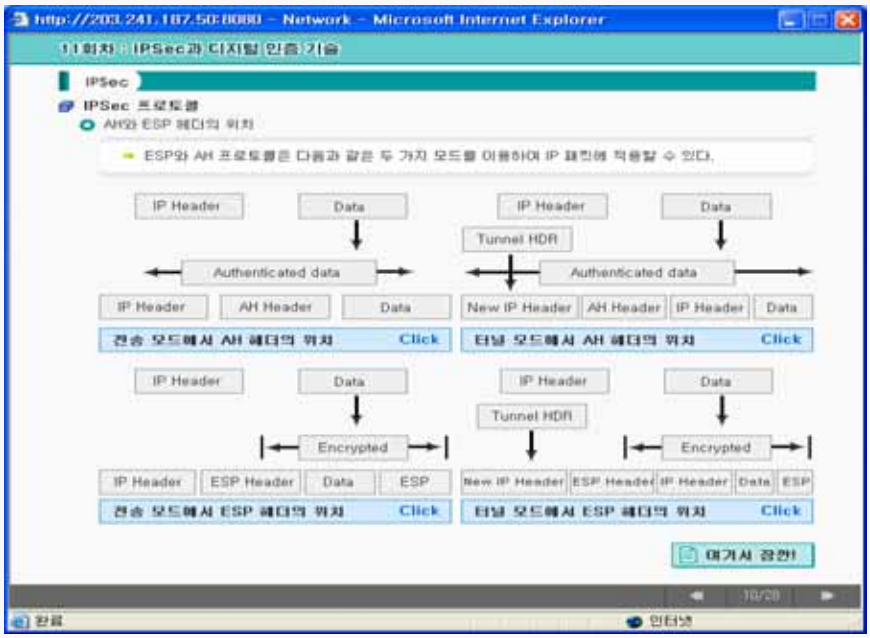

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
IPSec 프로토콜
ESP (Encapsulating Security Payload)
ESP는 다음과 같은 보안 서비스를 제공한다.
* 기밀성
* 데이터 근원지 인증
* 비 연결형 무결성
* 리플레이 방지 (anti-replay) 서비스
* 트래픽 흐름 (traffic flow) 분석 저지를 통한 제한적 의미의 트래픽 흐름에 대한 기밀성
데이터 근원지 인증과 비 연결형 무결성은 같이 제공되는 서비스이고,
기밀성 서비스 옵션과 함께 옵션으로 제공된다.
리플레이 방지 서비스는 데이터 근원지 인증 서비스가 선택되어 있으면 선택할 수 있다.
트래픽 흐름 기밀성은 트래픽 송신자와 수신자 패턴을 알 수 있는 보안 게이트웨이에 구현할 경우 가장 효과적이다.
참고
제공할 보안 기능 및 서비스는 초기에 SA (Security Association)를 설정할 때 선택한 옵션과 구현 상황에 따라 결정된다.
기밀성은 다른 서비스와는 독립적으로 선택될 수 있다.
그러나 ESP에, 또는 AH에 분리하여, 무결성/인증 서비스 지원 없이 기밀성 서비스를 사용하게 되면 해당 트래픽은 특정 형태의 공격에 노출될 수 있다.
참고
리플레이 방지 서비스의 선택은 어디까지나 수신 측의 분별 능력에 따른다. 즉, 비록 디폴트로는 송신 측에서 리플레이 방지 서비스에 사용되는 시퀀스 번호를 증가하도록 하고 있지만, 수신 측이 시퀀스 번호를 확인할 수 있어야만 서비스가 유효한 것이다.
주의
기밀성 서비스와 인증 서비스가 모두 선택 옵션이기는 하지만 적어도 둘 중 하나는 선택해야 한다.
여기서 잠깐!
완료
인터넷

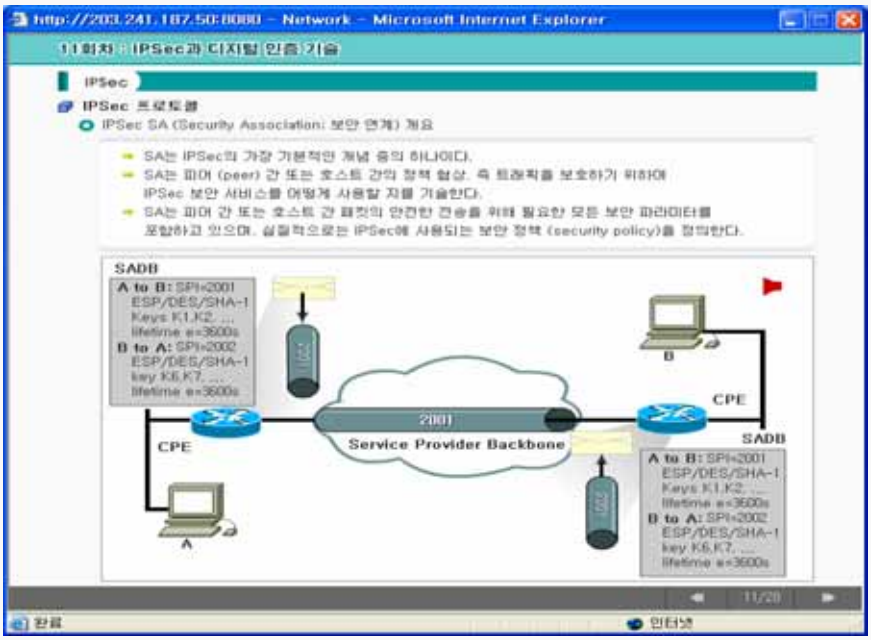

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
IPSec 프로토콜
ESP 프로토콜 헤더 구조
ESP 패킷 헤더 형식은 아래 그림과 같다.
헤더 내 필드 중 가장 중요한 값 중 하나는 SPI (Security Parameters Index)인데,
SPI는 라우터로 하여금 두 개의 IPSec 장치 간의 현재의 SA (Security Association)를
추적할 수 있도록 해준다.
암호화는 DES나 3DES를 이용하여 수행한다.
Security Parameter Index (SPI)
Sequence Number Field
Initialization Vector
Payload Data
Padding (if any)
Payload Length
Next Header
Authentication Data
여기서 잠깐!
참고
옵션 사항인 인증과 무결성 서비스는 SHA-1이나 MD5를
이용한 HMAC에 의해 제공된다.
SA (Security Association)에 포함된 두 가지 키 유형은
다음과 같다.
- 암호화 세션 키
- HMAC 세션 키
완료
인터넷

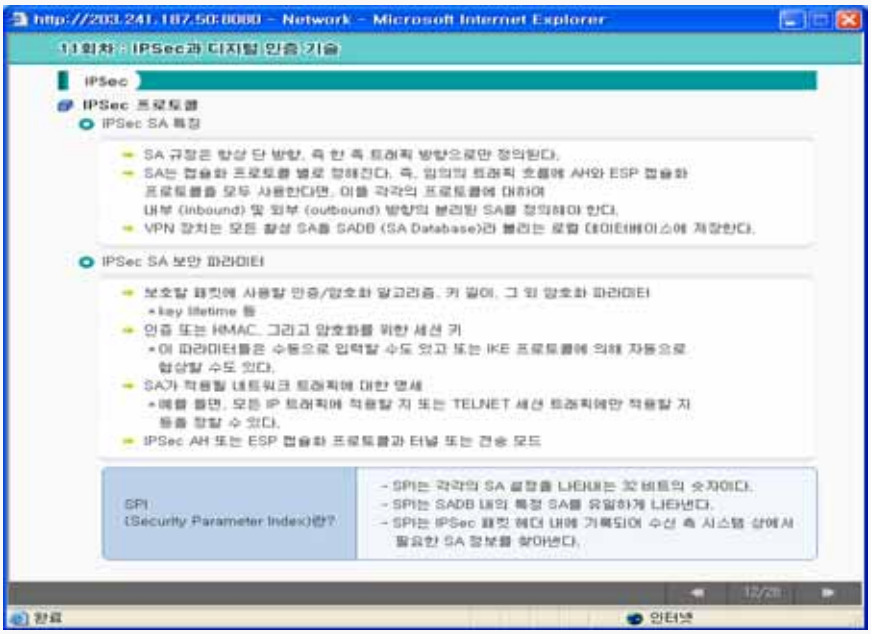

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
IPSec 프로토콜
AH와 ESP의 특징 비교
앞에서 살펴본 두 가지 IPSec 보안 프로토콜의 주요 특징을 비교/요약하면 다음과 같다.
AH 프로토콜
- 모든 데이터가 평문으로 전송된다.
- 데이터 무결성을 지원한다.
- 데이터 근원지 인증 기능을 제공한다.
- 즉, 패킷이 상대 라우터 (peer router)에서
발생되었음을 확인한다.
- 키 해시 (keyed-hash) 메커니즘을 사용한다.
- 기밀성을 지원하지 않는다.
즉, 암호화를 하지 않는다.
- 리플레이 방지 서비스는 옵션이다.
ESP 프로토콜
- 데이터 페이로드를 암호화한다.
- 제한적 의미의 트래픽 흐름 기밀성을 지원한다.
- 데이터 기밀성을 지원한다 (암호화).
- 데이터 무결성을 지원한다.
- 데이터 근원지 인증은 옵션이다.
- 리플레이 방지 서비스를 제공한다.
- IP 헤더를 보호하지 않는다.
완료
인터넷

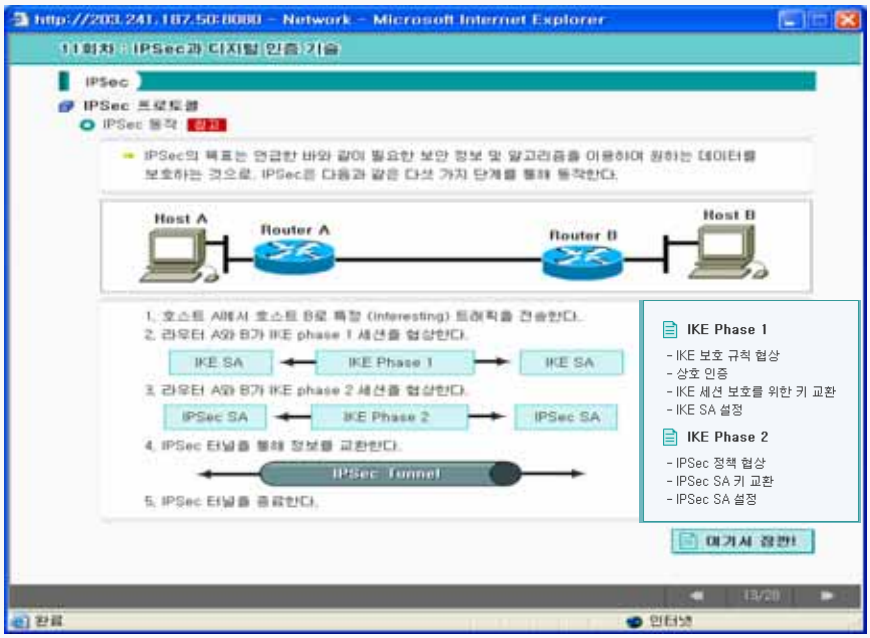

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
IPSec 프로토콜
IPSec 모드
ESP와 AH 프로토콜은 다음과 같은 두 가지 모드를 이용하여 IP 패킷에 적용할 수 있다.
전송 모드 (transport mode)
- 전송 모드에서는 전송 계층 이상의 계층에 대해서만 보안 기능이 제공된다.
- 전송 모드는 패킷의 페이로드를 보호하지만 원래의 IP 주소는 평문으로 전송한다.
- 인터넷에서 패킷에 대한 경로 선정을 위해서 원래의 IP 주소가 사용된다.
터널 모드 (tunnel mode)
- 터널 모드에서는 원래의 IP 패킷 전체에 대한 보안 기능을 제공한다.
- 터널 모드는 원래의 IP 패킷을 암호화한 후, 암호화한 패킷은 재차 또 다른 IP 패킷으로 캡슐화한다.
- 인터넷에서 패킷에 대한 경로 선정을 위해서 새로 추가된 바깥쪽의 IP 주소가 사용된다.
Tunnel Mode
Joe's PC
HR Server
Transport Mode
9/20
완료
인터넷

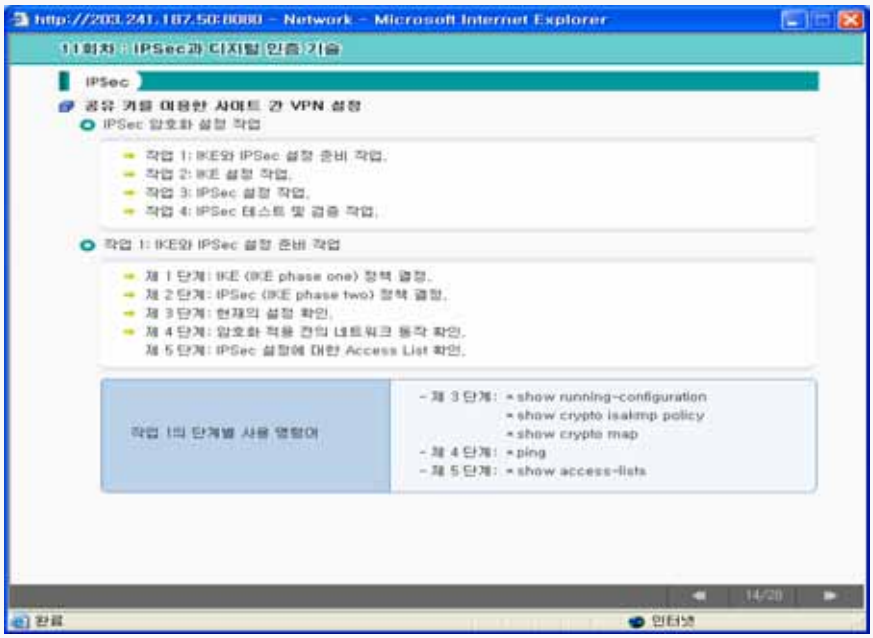

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
설정 작업
라우터에 IOS Firewall IDS를 설정하여 Cisco Secure IDS Director로 alarm을 통보하기 위해서는 다음과 같은 작업을 수행하여야 한다.
Cisco Firewall IDS 설정 작업 순서
1. IOS Firewall IDS 초기화
2. Signature 설정 (configure), 해제 (disable), 제외 (exclude)
3. 감사 규칙의 생성과 적용
4. 설정 확인
5. IDS Director Map에 IOS Firewall IDS 추가
IOS Firewall IDS 초기화
통보 유형 (Notification Type) 설정 명령어
Router(config)#ip audit notify (nr-director|log)
Alarm 통보 방법을 지정하기 위한 전역 설정 명령어이다.
로그 (log)는 VMS 보안 모니터 서버, 라우터의 내부 로그, 또는 Syslog 서버와 같은 IDS 관리 플랫폼으로 보내질 수 있다.
통보 유형 설정 예
ex) Router(config)# ip audit notify nr-director
Router(config)# ip audit notify log
해 설
9/20
완료
인터넷

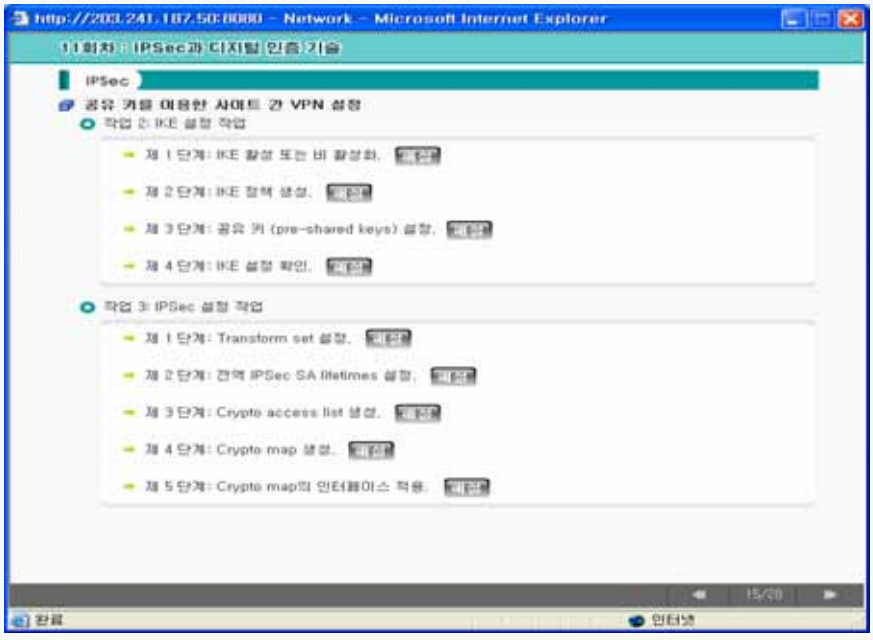

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
IPSec 프로토콜
AH와 ESP 헤더의 위치
ESP와 AH 프로토콜은 다음과 같은 두 가지 모드를 이용하여 IP 패킷에 적용할 수 있다.
IP Header
Data
Authenticated data
AH Header
New IP Header
Tunnel HDR
전송 모드에서 AH 헤더의 위치
Click
터널 모드에서 AH 헤더의 위치
Encrypted
ESP Header
ESP
전송 모드에서 ESP 헤더의 위치
터널 모드에서 ESP 헤더의 위치
여기서 끝한!
완료
인터넷

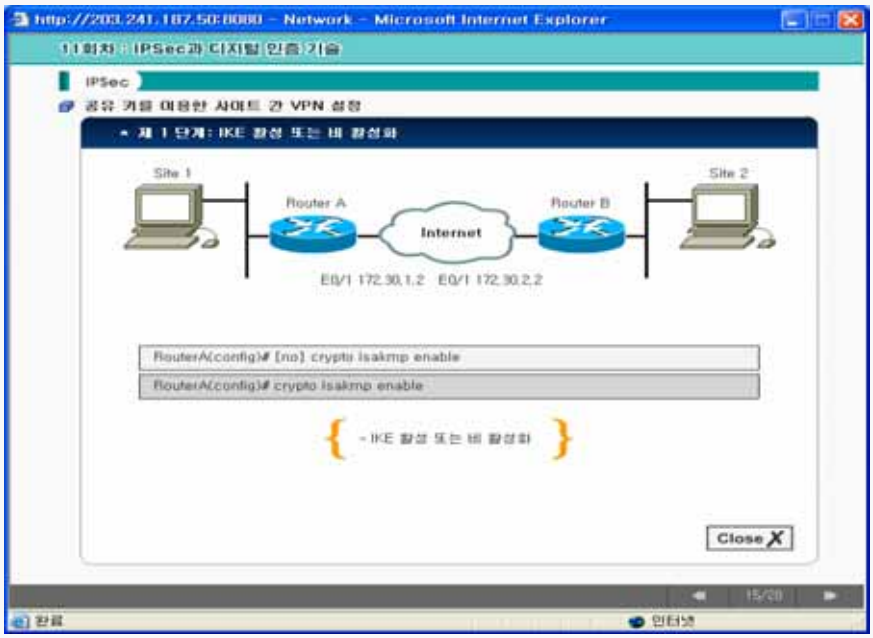

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
IPSec 프로토콜
IPSec SA (Security Association: 보안 연계) 개요
SA는 IPSec의 가장 기본적인 개념 중의 하나이다.
SA는 피어 (peer) 간 또는 호스트 간의 정책 협상, 즉 트래픽을 보호하기 위하여 IPSec 보안 서비스를 어떻게 사용할 지를 기술한다.
SA는 피어 간 또는 호스트 간 패킷의 안전한 전송을 위해 필요한 모든 보안 파라미터를 포함하고 있으며, 실질적으로는 IPSec에 사용되는 보안 정책 (security policy)을 정의한다.
SADB
A to B: SPI=2001
ESP/DES/SHA-1
Keys K1,K2, ...
lifetime e=3600s
B to A: SPI=2002
ESP/DES/SHA-1
key K6,K7, ...
lifetime e=3600s
CPE
2001
Service Provider Backbone
A
B
완료
인터넷

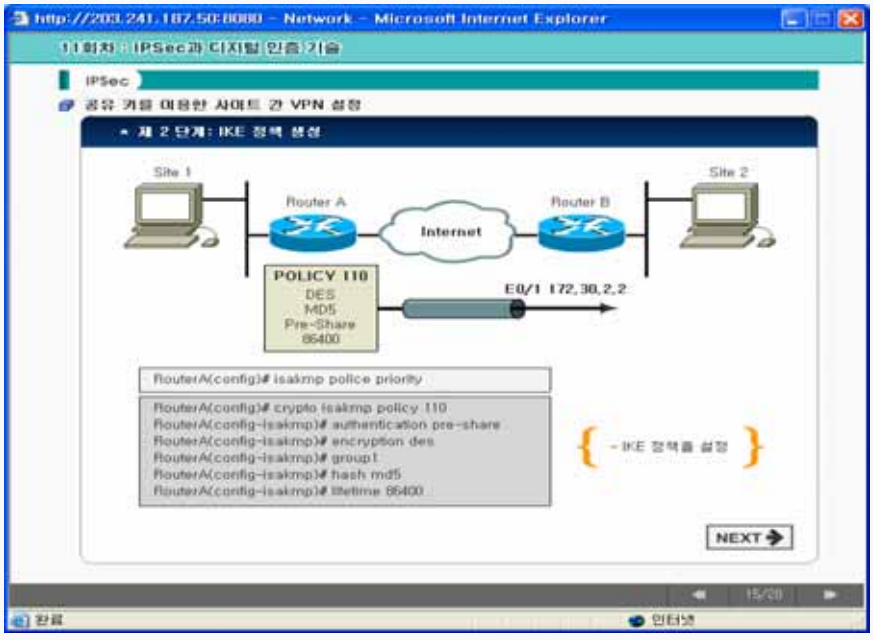

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
IPSec 프로토콜
IPSec SA 특징
SA 규정은 항상 단 방향, 즉 한 쪽 트래픽 방향으로만 정의된다.
SA는 캡슐화 프로토콜 별로 정해진다. 즉, 임의의 트래픽 흐름에 AH와 ESP 캡슐화 프로토콜을 모두 사용한다면, 이들 각각의 프로토콜에 대하여 내부 (inbound) 및 외부 (outbound) 방향의 분리된 SA를 정의해야 한다.
VPN 장치는 모든 활성 SA를 SADB (SA Database)라 불리는 로컬 데이터베이스에 저장한다.
IPSec SA 보안 파라미터
보호할 패킷에 사용할 인증/암호화 알고리즘, 키 길이, 그 외 암호화 파라미터
* key lifetime 등
인증 또는 HMAC, 그리고 암호화를 위한 세션 키
* 이 파라미터들은 수동으로 입력할 수도 있고 또는 IKE 프로토콜에 의해 자동으로 협상할 수도 있다.
SA가 적용될 네트워크 트래픽에 대한 명세
* 예를 들면, 모든 IP 트래픽에 적용할 지 또는 TELNET 세션 트래픽에만 적용할 지 등을 정할 수 있다.
IPSec AH 또는 ESP 캡슐화 프로토콜과 터널 또는 전송 모드
SPI (Security Parameter Index)란?
- SPI는 각각의 SA 설정을 나타내는 32 비트의 숫자이다.
- SPI는 SADB 내의 특정 SA를 유일하게 나타낸다.
- SPI는 IPSec 패킷 헤더 내에 기록되어 수신 측 시스템 상에서 필요한 SA 정보를 찾아낸다.
12/20
완료
인터넷

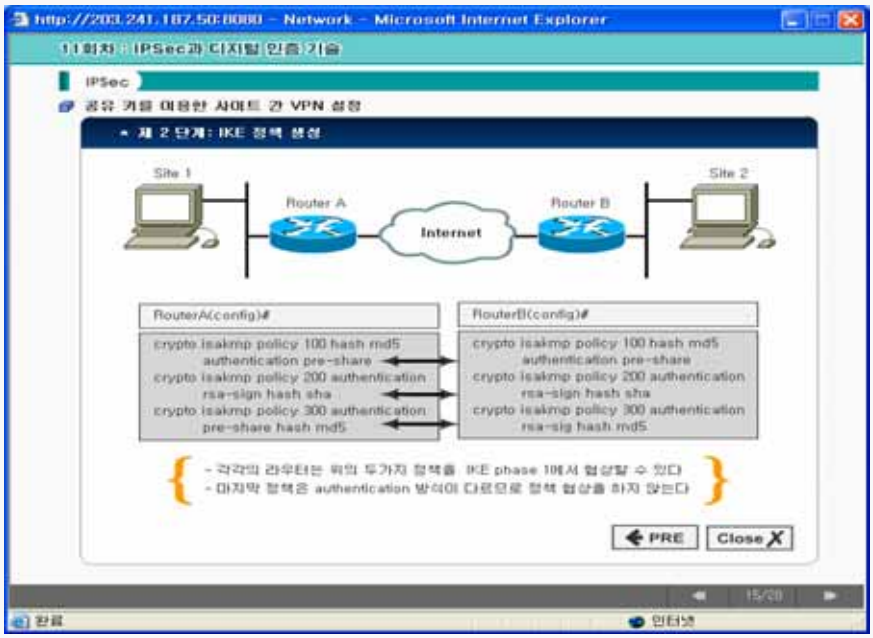

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
IPSec 프로토콜
IPSec 동작
IPSec의 목표는 언급한 바와 같이 필요한 보안 정보 및 알고리즘을 이용하여 원하는 데이터를 보호하는 것으로, IPSec은 다음과 같은 다섯 가지 단계를 통해 동작한다.
Host A
Router A
Router B
Host B
1. 호스트 A에서 호스트 B로 특정 (interesting) 트래픽을 전송한다.
2. 라우터 A와 B가 IKE phase 1 세션을 협상한다.
IKE SA
IKE Phase 1
IKE SA
3. 라우터 A와 B가 IKE phase 2 세션을 협상한다.
IPSec SA
IKE Phase 2
IPSec SA
4. IPSec 터널을 통해 정보를 교환한다.
IPSec Tunnel
5. IPSec 터널을 종료한다.
IKE Phase 1
- IKE 보호 규칙 협상
- 상호 인증
- IKE 세션 보호를 위한 키 교환
- IKE SA 설정
IKE Phase 2
- IPSec 정책 협상
- IPSec SA 키 교환
- IPSec SA 설정
여기서 끝!!
13/20
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
IPSec 암호화 설정 작업
작업 1: IKE와 IPSec 설정 준비 작업.
작업 2: IKE 설정 작업.
작업 3: IPSec 설정 작업.
작업 4: IPSec 테스트 및 검증 작업.
작업 1: IKE와 IPSec 설정 준비 작업
제 1 단계: IKE (IKE phase one) 정책 결정.
제 2 단계: IPSec (IKE phase two) 정책 결정.
제 3 단계: 현재의 설정 확인.
제 4 단계: 암호화 적용 간의 네트워크 동작 확인.
제 5 단계: IPSec 설정에 대한 Access List 확인.
작업 1의 단계별 사용 명령어
- 제 3 단계: • show running-configuration
• show crypto isakmp policy
• show crypto map
- 제 4 단계: • ping
- 제 5 단계: • show access-lists
14/20
완료
인터넷

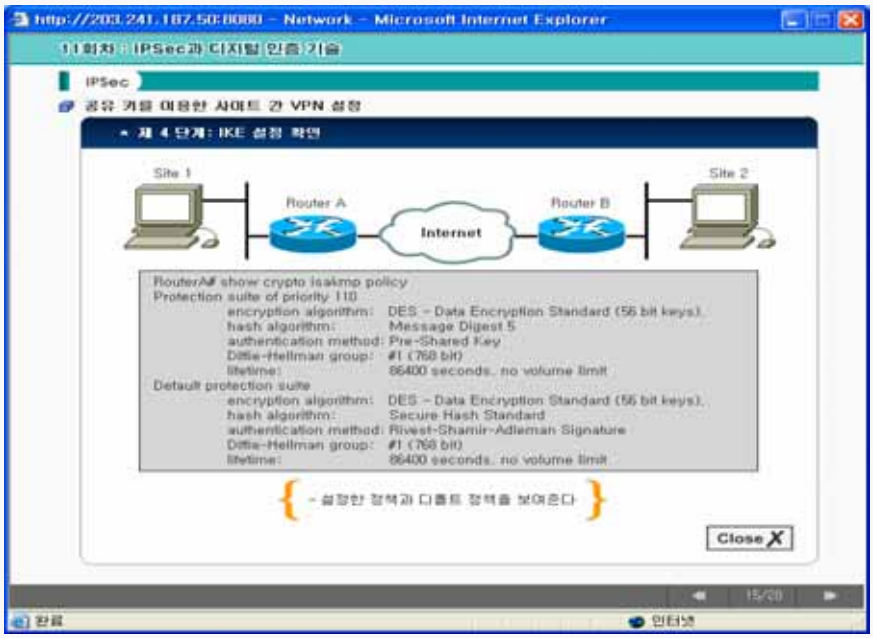

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
작업 2: IKE 설정 작업
제 1 단계: IKE 활성 또는 비 활성화.
제 2 단계: IKE 정책 생성.
제 3 단계: 공유 키 (pre-shared keys) 설정.
제 4 단계: IKE 설정 확인.
작업 3: IPSec 설정 작업
제 1 단계: Transform set 설정.
제 2 단계: 관련 IPSec SA lifetimes 설정.
제 3 단계: Crypto access list 생성.
제 4 단계: Crypto map 생성.
제 5 단계: Crypto map의 인터페이스 적용.
15/20
완료
인터넷

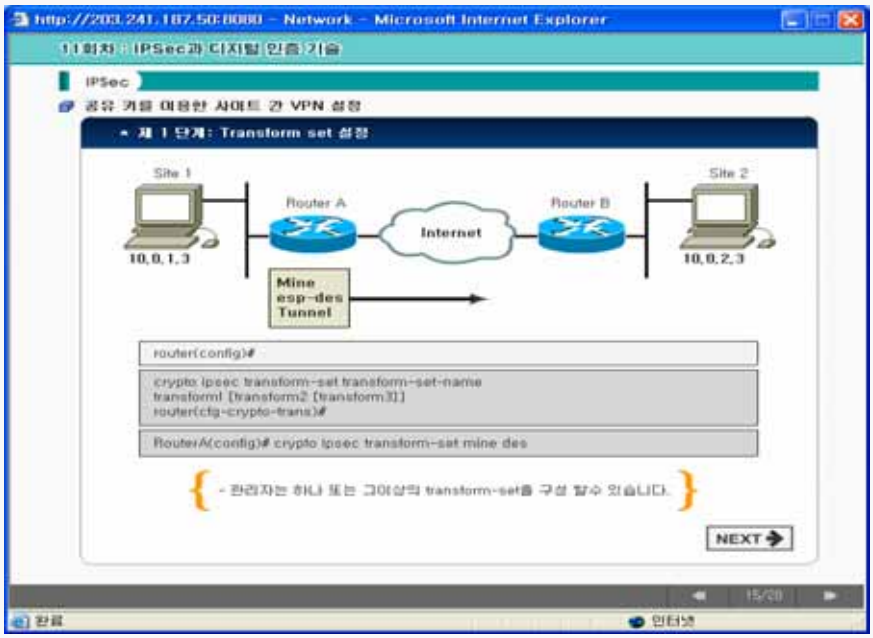

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
제 1 단계: IKE 활성 또는 비 활성화
Site 1
Router A
Internet
Router B
Site 2
E0/1 172.30.1.2
E0/1 172.30.2.2
RouterA(config)# [no] crypto isakmp enable
RouterA(config)# crypto isakmp enable
- IKE 활성 또는 비 활성화
Close
15/20
완료
인터넷

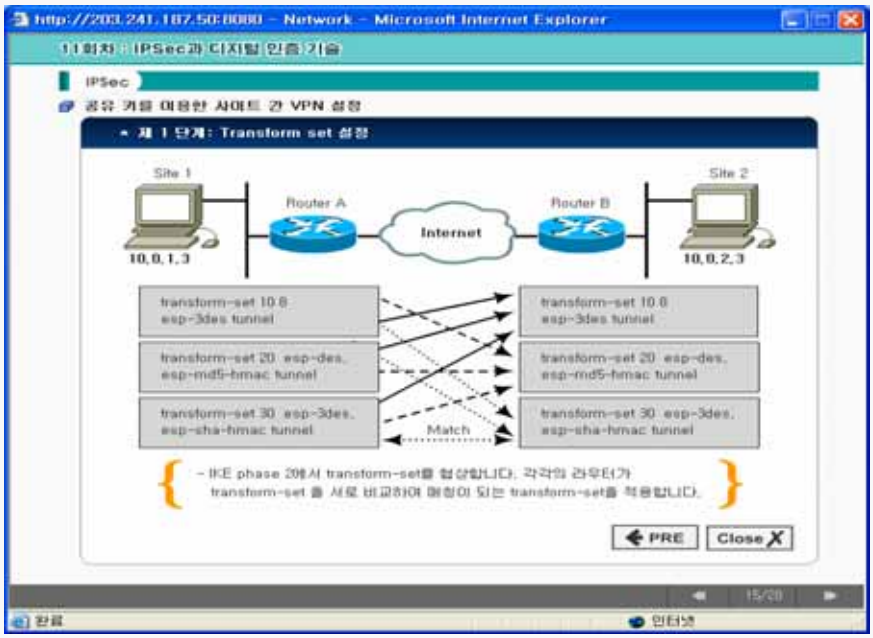

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
제 2 단계: IKE 정책 설정
Site 1
Router A
Internet
Router B
Site 2
POLICY 110
DES
MD5
Pre-Share
86400
E0/1 172.30.2.2
RouterA(config)# isakmp police priority
RouterA(config)# crypto isakmp policy 110
RouterA(config-isakmp)# authentication pre-share
RouterA(config-isakmp)# encryption des
RouterA(config-isakmp)# group1
RouterA(config-isakmp)# hash md5
RouterA(config-isakmp)# lifetime 86400
- IKE 정책을 설정
NEXT
15/20
완료
인터넷

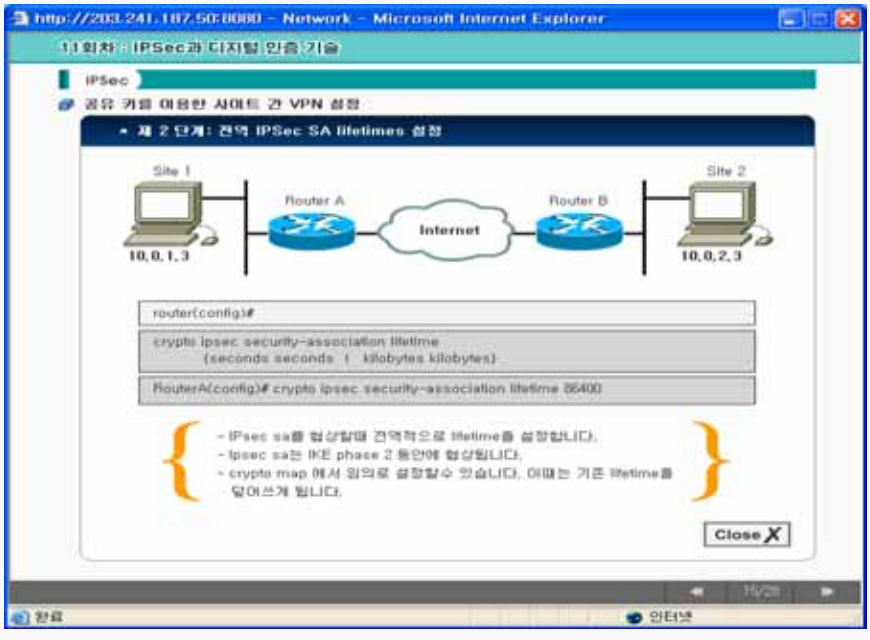

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
• 제 2 단계: IKE 정책 설정
Site 1
Router A
Internet
Router B
Site 2
RouterA(config)#
crypto isakmp policy 100 hash md5
authentication pre-share
crypto isakmp policy 200 authentication
rsa-sign hash sha
crypto isakmp policy 300 authentication
pre-share hash md5
RouterB(config)#
crypto isakmp policy 100 hash md5
authentication pre-share
crypto isakmp policy 200 authentication
rsa-sign hash sha
crypto isakmp policy 300 authentication
rsa-sig hash md5
- 각각의 라우터는 위의 두가지 정책을 IKE phase 1에서 협상할 수 있다
- 마지막 정책은 authentication 방식이 다르므로 정책 협상을 하지 않는다
PRE
Close
15/20
완료
인터넷

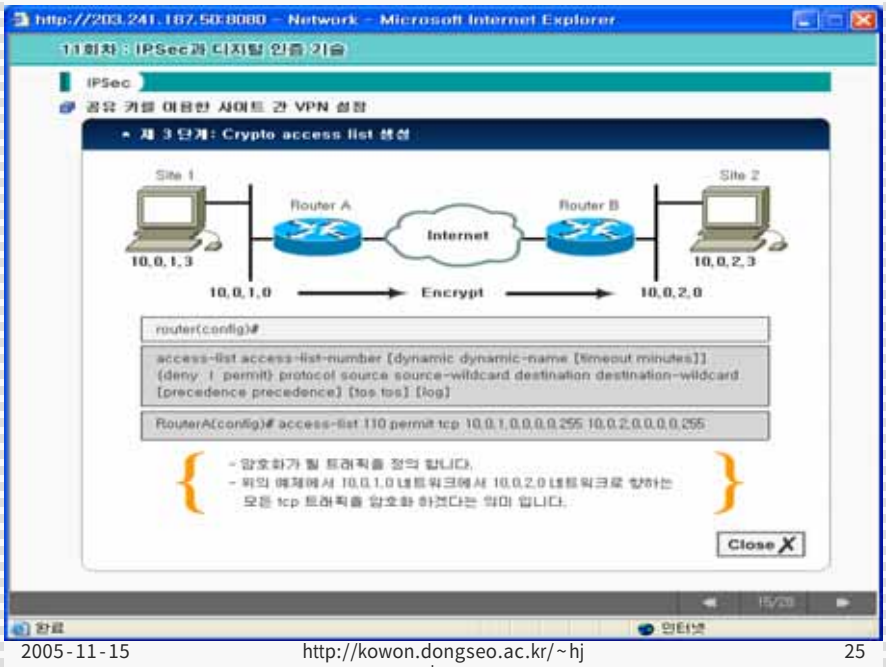

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
• 제 3 단계: 공유 키 (pre-shared keys) 설정
Site 1
Router A
Internet
Router B
Site 2
Pre-sharde key Cisco 1234
172.30.2.2
RouterA(config)# crypto isakmp key cisco1234 address 172.30.2.2
crypto isakmp key keystring address peer-address
crypto isakmp key keystring hostname peer-hostname
명 령 어
설 명
Keystring
Pre-shared key를 정의 합니다. 양측 피어 라우터가 동일하게 설정이 되어야만 합니다.
Peer-address
피어 라우터의 IP address를 설정 합니다.
Peer-hostname
피어 라우터의 호스트 이름으로 설정합니다. 이와 같은 경우에는 라우터의 도메인이름과 같이 사용되어집니다. (예. RouterA.domain.com)
Close
15/20
완료
인터넷

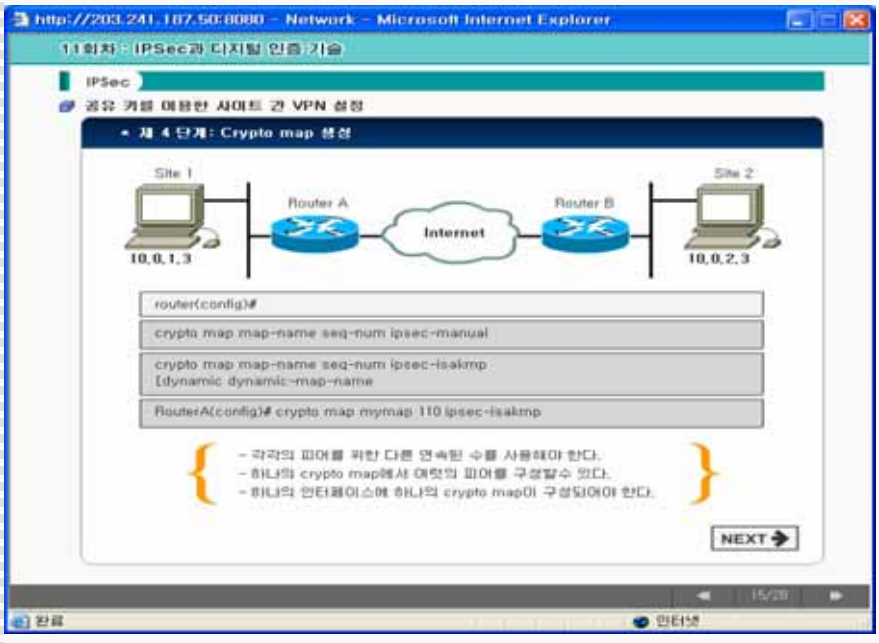

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
제 4 단계: IKE 설정 확인
Site 1
Router A
Internet
Router B
Site 2
RouterA# show crypto isakmp policy
Protection suite of priority 110
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
- 설정한 정책과 디폴트 정책을 보여준다
Close
15/20
완료
인터넷

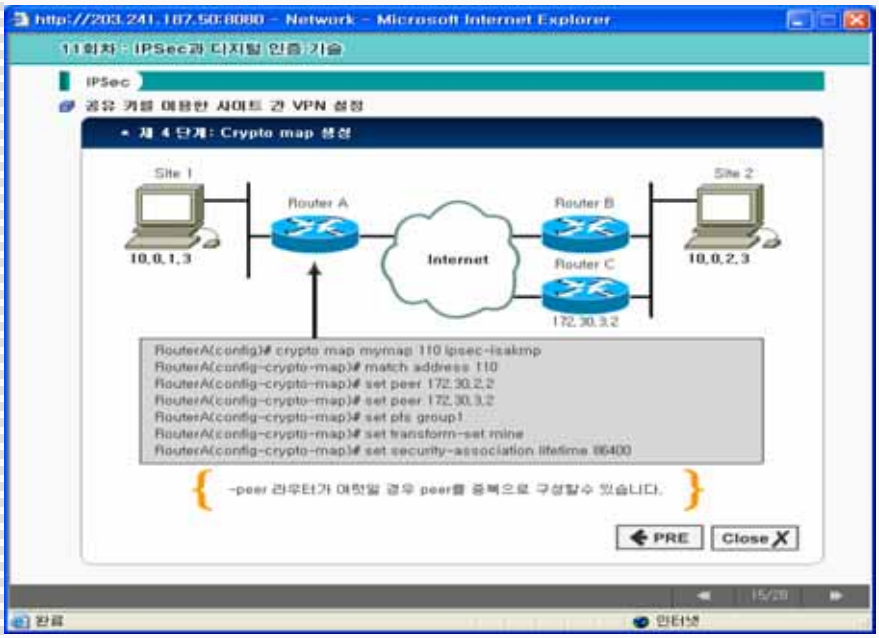

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
제 1 단계: Transform set 설정
Site 1
Router A
Internet
Router B
Site 2
10.0.1.3
10.0.2.3
Mine
esp-des
Tunnel
router(config)#
crypto ipsec transform-set transform-set-name
transform1 [transform2 [transform3]]
router(cfg-crypto-trans)#
RouterA(config)# crypto ipsec transform-set mine des
- 관리자는 하나 또는 그이상의 transform-set을 구성 할수 있습니다.
NEXT
15/20
완료
인터넷

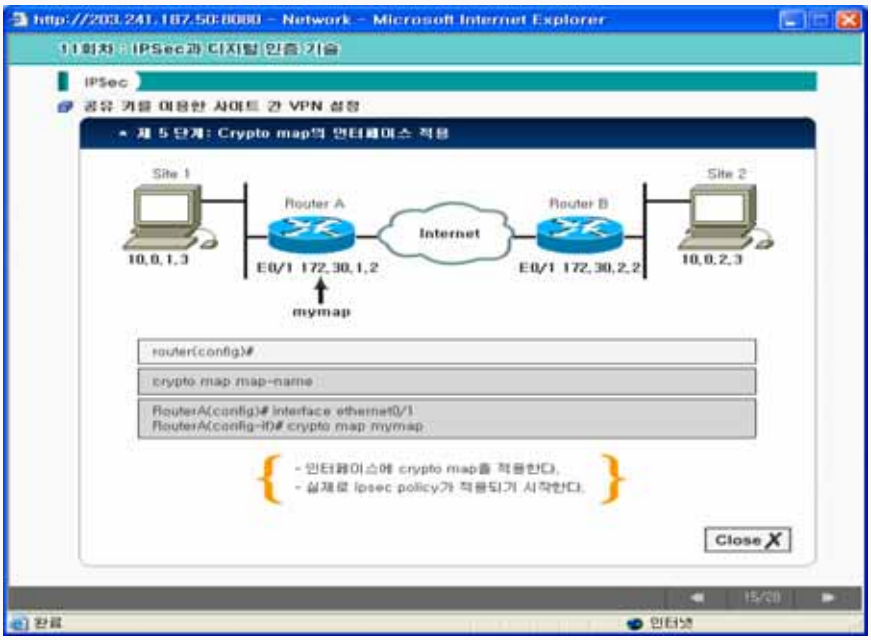

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
- 제 1 단계: Transform set 설정
Site 1
Router A
Internet
Router B
Site 2
10.0.1.3
10.0.2.3
transform-set 10 esp-3des tunnel
transform-set 20 esp-des, esp-md5-hmac tunnel
transform-set 30 esp-3des, esp-sha-hmac tunnel
Match
- IKE phase 2에서 transform-set를 협상합니다. 각각의 라우터가 transform-set 을 서로 비교하여 매칭이 되는 transform-set를 적용합니다.
PRE
Close
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
- 제 2 단계: 전역 IPSec SA lifetimes 설정
Site 1
Router A
Internet
Router B
Site 2
10.0.1.3
10.0.2.3
router(config)#
crypto ipsec security-association lifetime {seconds seconds | kilobytes kilobytes}
RouterA(config)# crypto ipsec security-association lifetime 86400
- IPsec sa를 협상할때 전역적으로 lifetime을 설정합니다.
- Ipsec sa는 IKE phase 2 동안에 협상됩니다.
- crypto map 에서 임의로 설정할수 있습니다. 이때는 기존 lifetime을 덮어쓰게 됩니다.
Close
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
• 제 3 단계: Crypto access list 생성
Site 1
Router A
Internet
Router B
Site 2
10.0.1.3
10.0.2.3
10.0.1.0
Encrypt
10.0.2.0
router(config)#
access-list access-list-number {dynamic dynamic-name [timeout minutes]}
{deny | permit} protocol source source-wildcard destination destination-wildcard
[precedence precedence] [tos tos] [log]
RouterA(config)# access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
- 암호화가 될 트래픽을 정의 합니다.
- 위의 예제에서 10.0.1.0 네트워크에서 10.0.2.0 네트워크로 향하는
모든 tcp 트래픽을 암호화 하겠다는 의미 입니다.
Close
15/28
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
• 제 4 단계: Crypto map 생성
Site 1
Router A
Internet
Router B
Site 2
10.0.1.3
10.0.2.3
router(config)#
crypto map map-name seq-num ipsec-manual
crypto map map-name seq-num ipsec-isakmp
[dynamic dynamic-map-name]
RouterA(config)# crypto map mymap 110 ipsec-isakmp
- 각각의 피어를 위한 다른 연속된 수를 사용해야 한다.
- 하나의 crypto map에서 여럿의 피어를 구성할수 있다.
- 하나의 인터페이스에 하나의 crypto map이 구성되어야 한다.
NEXT
15/28
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
• 제 4 단계: Crypto map 설정
Site 1
Router A
Internet
Router B
Router C
Site 2
10.0.1.3
10.0.2.3
172.30.3.2
RouterA(config)# crypto map mymap 110 ipsec-isakmp
RouterA(config-crypto-map)# match address 110
RouterA(config-crypto-map)# set peer 172.30.2.2
RouterA(config-crypto-map)# set peer 172.30.3.2
RouterA(config-crypto-map)# set pfs group1
RouterA(config-crypto-map)# set transform-set mine
RouterA(config-crypto-map)# set security-association lifetime 86400
-peer 라우터가 여럿일 경우 peer를 중복으로 구성할수 있습니다.
PRE
Close
15/28
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
• 제 5 단계: Crypto map의 인터페이스 적용
Site 1
Router A
Internet
Router B
Site 2
10.0.1.3
E0/1 172.30.1.2
E0/1 172.30.2.2
10.0.2.3
mymap
router(config)#
crypto map map-name
RouterA(config)# interface ethernet0/1
RouterA(config-if)# crypto map mymap
- 인터페이스에 crypto map을 적용한다.
- 실제로 ipsec policy가 적용되기 시작한다.
Close
15/28
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
IPSec
공유 키를 이용한 사이트 간 VPN 설정
작업 4: IPSec 테스트 및 검증 작업
IKE 정책 설정 확인
Transform set 설정 확인
IPSec SA의 현재 상태 확인
Crypto map 설정 확인
IPSec 이벤트에 대한 디버그 출력 활성화
ISAKMP 이벤트에 대한 디버그 출력 활성화
완료
인터넷

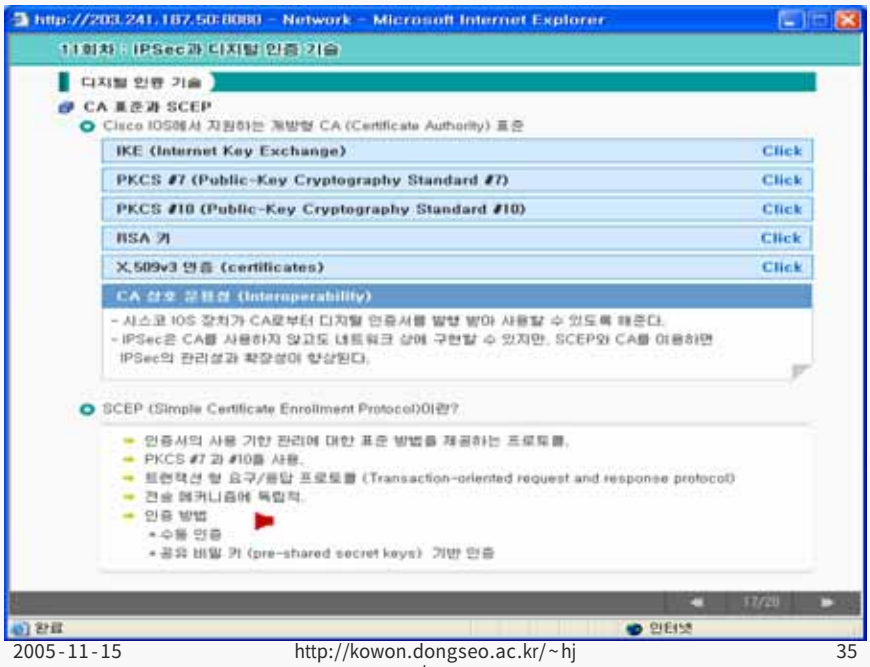

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
디지털 인증 기술
CA 표준과 SCEP
Cisco IOS에서 지원하는 계층형 CA (Certificate Authority) 표준
IKE (Internet Key Exchange)
PKCS #7 (Public-Key Cryptography Standard #7) Click
PKCS #10 (Public-Key Cryptography Standard #10) Click
RSA 키 Click
X.509v3 인증 (certificates) Click
CA 상호 운용성 (Interoperability) Click
SCEP (Simple Certificate Enrollment Protocol)이란?
인증서의 사용 기한 관리에 대한 표준 방법을 제공하는 프로토콜.
PKCS #7 과 #10을 사용.
트랜잭션 형 요구/응답 프로토콜 (Transaction-oriented request and response protocol)
전송 메커니즘에 독립적.
인증 방법
수동 인증
공유 비밀 키 (pre-shared secret keys) 기반 인증
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
디지털 인증 기술
CA 표준과 SCEP
Cisco IOS에서 지원하는 계층형 CA (Certificate Authority) 표준
IKE (Internet Key Exchange) Click
PKCS #7 (Public-Key Cryptography Standard #7)
RSA Data Security 사의 표준으로 인증서 등록 (certificate enrollment) 메시지에 대한
암호화/서명/패키지를 위해 사용된다.
PKCS #10 (Public-Key Cryptography Standard #10) Click
RSA 키 Click
X.509v3 인증 (certificates) Click
CA 상호 운용성 (Interoperability) Click
SCEP (Simple Certificate Enrollment Protocol)이란?
인증서의 사용 기한 관리에 대한 표준 방법을 제공하는 프로토콜.
PKCS #7 과 #10을 사용.
트랜잭션 형 요구/응답 프로토콜 (Transaction-oriented request and response protocol)
간송 메커니즘에 독립적.
인증 방법
- 수동 인증
- 공유 비밀 키 (pre-shared secret keys) 기반 인증
12/28
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
디지털 인증 기술
CA 표준과 SCEP
Cisco IOS에서 지원하는 계층형 CA (Certificate Authority) 표준
IKE (Internet Key Exchange) Click
PKCS #7 (Public-Key Cryptography Standard #7) Click
PKCS #10 (Public-Key Cryptography Standard #10)
인증서 요구 (certificate request)를 위한 RSA Data Security 사의 표준 구문 (standard syntax).
RSA 키 Click
X.509v3 인증 (certificates) Click
CA 상호 운용성 (Interoperability) Click
SCEP (Simple Certificate Enrollment Protocol)이란?
인증서의 사용 기한 관리에 대한 표준 방법을 제공하는 프로토콜.
PKCS #7 과 #10을 사용.
트랜잭션 형 요구/응답 프로토콜 (Transaction-oriented request and response protocol)
간송 메커니즘에 독립적.
인증 방법
- 수동 인증
- 공유 비밀 키 (pre-shared secret keys) 기반 인증
12/28
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
디지털 인증 기술
CA 표준과 SCEP
Cisco IOS에서 지원하는 계층형 CA (Certificate Authority) 표준
IKE (Internet Key Exchange) Click
PKCS #7 (Public-Key Cryptography Standard #7) Click
PKCS #10 (Public-Key Cryptography Standard #10) Click
RSA 키
- Ron Rivest, Adi Shamir, Leonard Adleman에 의해 개발된 공개 키 암호화 시스템.
- RSA 키는 공개 키와 개인 키 쌍으로 구성된다.
X.509v3 인증 (certificates) Click
CA 상호 운용성 (Interoperability) Click
SCEP (Simple Certificate Enrollment Protocol)이란?
인증서의 사용 기한 관리에 대한 표준 방법을 제공하는 프로토콜.
PKCS #7 과 #10을 사용.
트랜잭션 형 요구/응답 프로토콜 (Transaction-oriented request and response protocol)
간송 메커니즘에 독립적.
인증 방법
- 수동 인증
- 공유 비밀 키 (pre-shared secret keys) 기반 인증
12/28
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
디지털 인증 기술
CA 표준과 SCEP
Cisco IOS에서 지원하는 계층형 CA (Certificate Authority) 표준
IKE (Internet Key Exchange) Click
PKCS #7 (Public-Key Cryptography Standard #7) Click
PKCS #10 (Public-Key Cryptography Standard #10) Click
RSA 키 Click
X.509v3 인증 (certificates)
- 네트워킹 장치에 디지털 ID 카드를 제공함으로써 IPSec 보안 네트워크에 확장성을 지원하는 인증 기술.
- 통신 장치 간에는 디지털 인증서를 사용하여 상호 인증이 수행되므로,
공개 키를 수동으로 교환하거나 공유 키를 수동으로 지정할 필요가 없다.
- 디지털 인증서는 CA로부터 얻을 수 있다.
CA 상호 운용성 (Interoperability) Click
SCEP (Simple Certificate Enrollment Protocol)이란?
인증서의 사용 기한 관리에 대한 표준 방법을 제공하는 프로토콜.
PKCS #7 과 #10을 사용.
트랜잭션 형 요구/응답 프로토콜 (Transaction-oriented request and response protocol)
간송 메커니즘에 독립적.
인증 방법
- 수동 인증
- 공유 비밀 키 (pre-shared secret keys) 기반 인증
12/28
완료
인터넷



CA 서버

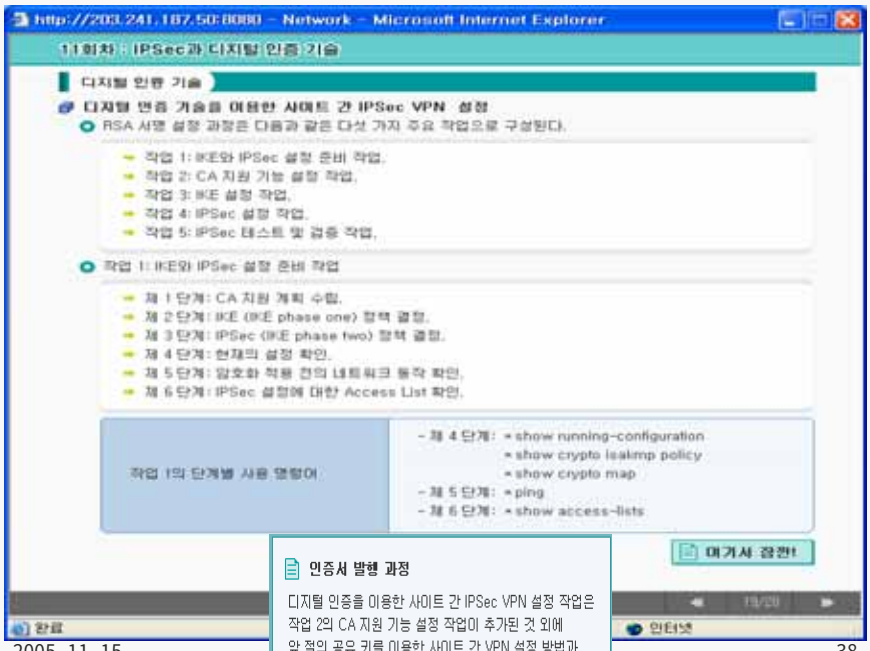
예를 들어 마이크로소프트 사는 윈도우 2000 CA 서버 내에 SCEP 지원 기능을 통합하였다. SCEP는 시스코 장치로 하여금 시스코의 모든 VPN 보안 솔루션에 대하여 마이크로소프트 인증 서비스로부터 인증서 및 인증서 폐지 정보를 얻을 수 있도록 도와준다.
단, SCEP 도구는 디폴트로 설치되지 않기 때문에 마이크로소프트 CA 서비스를 설치한 후 윈도우 2000 서버 리소스 키트를 사용하여 별도로 SCEP 도구를 설치해야 한다.

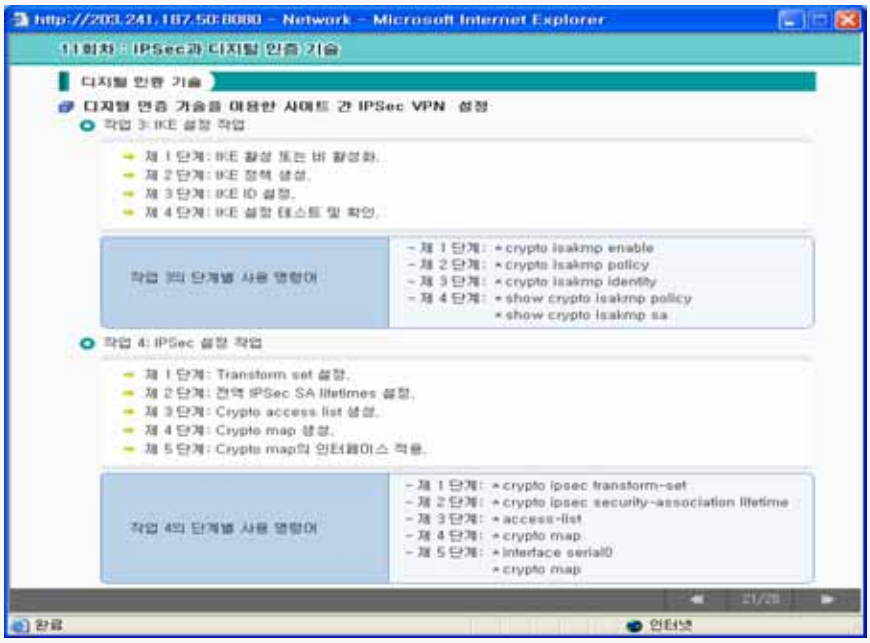
인증서 발행 과정

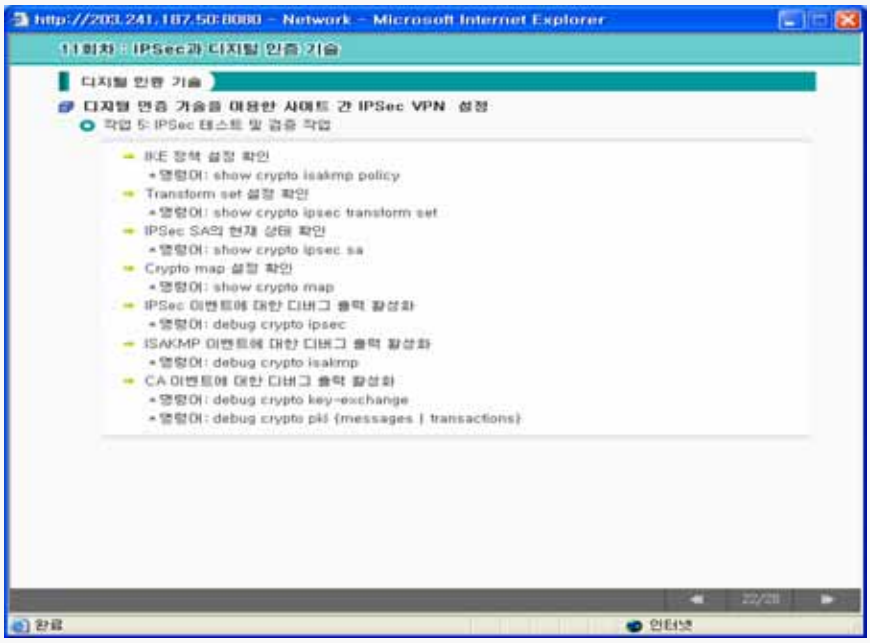
제 1 단계: CA 지원을 위한 라우터 설정.
제 2 단계: 라우터 상에 공개 키와 개인 키 쌍 발행.
제 3 단계: 라우터에 의한 CA 서버 인증.
- CA로 certificate request 전송.
- CA 인증서 발행
- CA 인증서를 라우터로 다운로드.
- CA fingerprint를 통한 CA 인증서 인증.

제 4 단계: 라우터에서 CA로 certificate request 전송.
제 5 단계: CA에서 ID 인증서 발행 및 서명.
제 6 단계: CA에서 라우터로 인증서 전송 및 CA 서버 내에 인증서 보관.
제 7 단계: 라우터에서 ID 인증서 확인 및 보관.


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
디지털 인증 기술
CA 서버와 인증서 발행 과정
CA 서버
삼지
시스코 라우터의 IOS 소프트웨어와 상호 운용이 가능한 대표적인 몇 가지 인증 기관은 다음과 같다.
• Entrust, VeriSign, Baltimore, Microsoft.
일부 CA 벤더는 시스코 라우터를 등록하기 위해 SCEP를 지원한다.
인증서 발행 과정
CA의 인증서 발행 과정은 보통 다음과 같은 절차를 통해 이루어진다.
CA 지원 설정
키 발행
CA 인증 요구
CA 인증
인증서 요구
ID 인증서 확인
CA 인증서 발행
CA 인증서 다운로드
ID 인증서 다운로드
ID 인증서 발행
여기서 잠깐!
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
디지털 인증 기술
디지털 인증 기술을 이용한 사이트 간 IPSec VPN 설정
RSA 서명 설정 과정은 다음과 같은 다섯 가지 주요 작업으로 구성된다.
작업 1: IKE와 IPSec 설정 준비 작업.
작업 2: CA 지원 기능 설정 작업.
작업 3: IKE 설정 작업.
작업 4: IPSec 설정 작업.
작업 5: IPSec 테스트 및 검증 작업.
작업 1: IKE와 IPSec 설정 준비 작업
제 1 단계: CA 지원 계획 수립.
제 2 단계: IKE (IKE phase one) 정책 결정.
제 3 단계: IPSec (IKE phase two) 정책 결정.
제 4 단계: 현재의 설정 확인.
제 5 단계: 암호화 적용 전의 네트워크 동작 확인.
제 6 단계: IPSec 설정에 대한 Access List 확인.
작업 1의 단계별 사용 명령어
- 제 4 단계: • show running-configuration
• show crypto isakmp policy
• show crypto map
- 제 5 단계: • ping
- 제 6 단계: • show access-lists
여기서 잠깐!
인증서 발행 과정
디지털 인증을 이용한 사이트 간 IPSec VPN 설정 작업은 작업 2의 CA 지원 기능 설정 작업이 추가된 것 외에 앞 절의 공유 키를 이용한 사이트 간 VPN 설정 방법과 크게 다르지 않음을 알 수 있다.
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
디지털 인증 기술
디지털 인증 기술을 이용한 사이트 간 IPSec VPN 설정
작업 3: IKE 설정 작업
제 1 단계: IKE 활성 또는 비 활성화.
제 2 단계: IKE 정책 생성.
제 3 단계: IKE ID 설정.
제 4 단계: IKE 설정 테스트 및 확인.
작업 3의 단계별 사용 명령어
- 제 1 단계: • crypto isakmp enable
- 제 2 단계: • crypto isakmp policy
- 제 3 단계: • crypto isakmp identity
- 제 4 단계: • show crypto isakmp policy
• show crypto isakmp sa
작업 4: IPSec 설정 작업
제 1 단계: Transform set 설정.
제 2 단계: 전역 IPSec SA lifetimes 설정.
제 3 단계: Crypto access list 생성.
제 4 단계: Crypto map 생성.
제 5 단계: Crypto map의 인터페이스 적용.
작업 4의 단계별 사용 명령어
- 제 1 단계: • crypto ipsec transform-set
- 제 2 단계: • crypto ipsec security-association lifetime
- 제 3 단계: • access-list
- 제 4 단계: • crypto map
- 제 5 단계: • interface serial0
• crypto map
21/28
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
11회차 : IPSec과 디지털 인증 기술
디지털 인증 기술
디지털 인증 기술을 이용한 사이트 간 IPSec VPN 설정
작업 5: IPSec 테스트 및 검증 작업
IKE 정책 설정 확인
• 명령어: show crypto isakmp policy
Transform set 설정 확인
• 명령어: show crypto ipsec transform set
IPSec SA의 현재 상태 확인
• 명령어: show crypto ipsec sa
Crypto map 설정 확인
• 명령어: show crypto map
IPSec 이벤트에 대한 디버그 출력 활성화
• 명령어: debug crypto ipsec
ISAKMP 이벤트에 대한 디버그 출력 활성화
• 명령어: debug crypto isakmp
CA 이벤트에 대한 디버그 출력 활성화
• 명령어: debug crypto key-exchange
• 명령어: debug crypto pki {messages | transactions}
22/28
완료
인터넷

End of Lecture