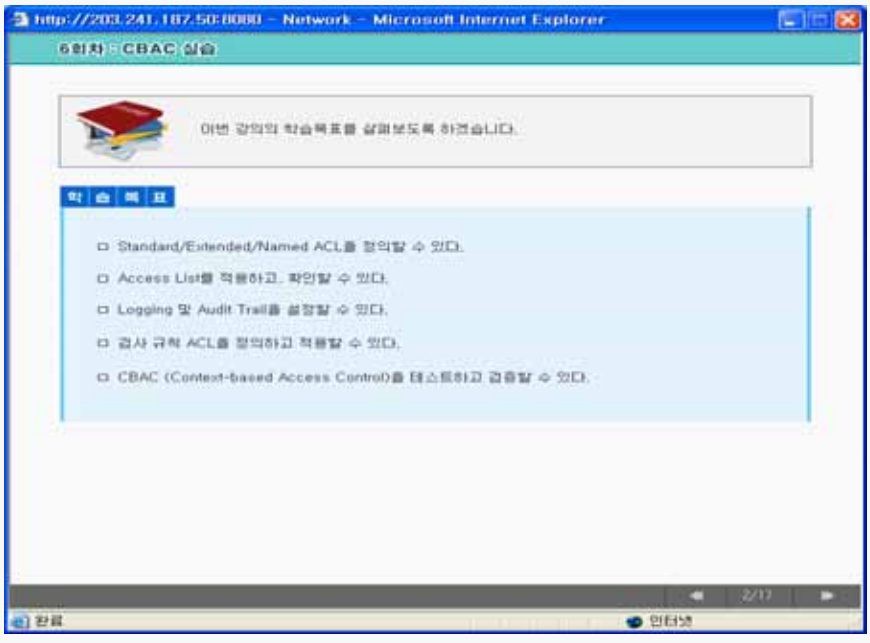
# FNS

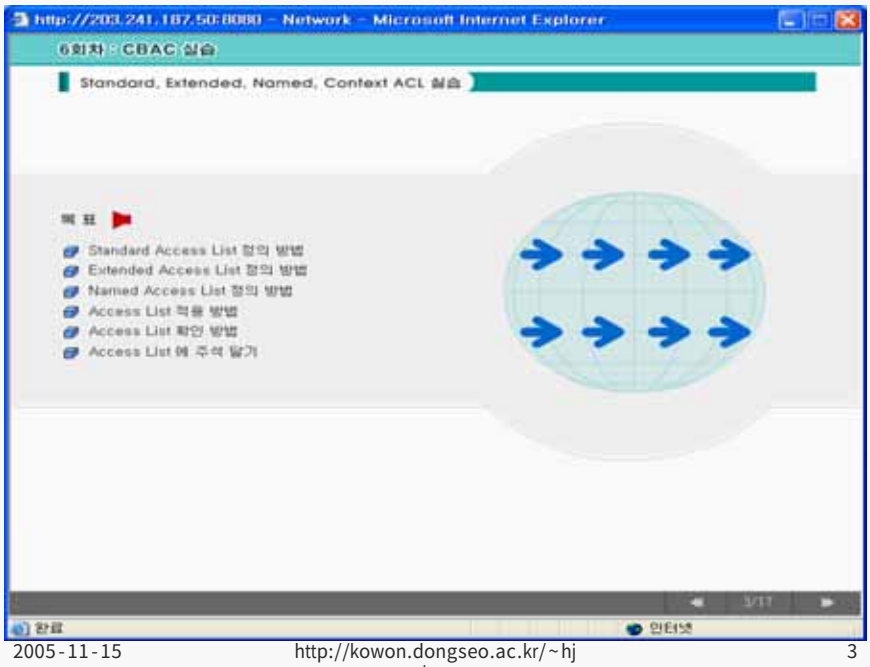
(Fundamental Network Security)

## Ch6. CBAC(Context-based Access Control) 실습

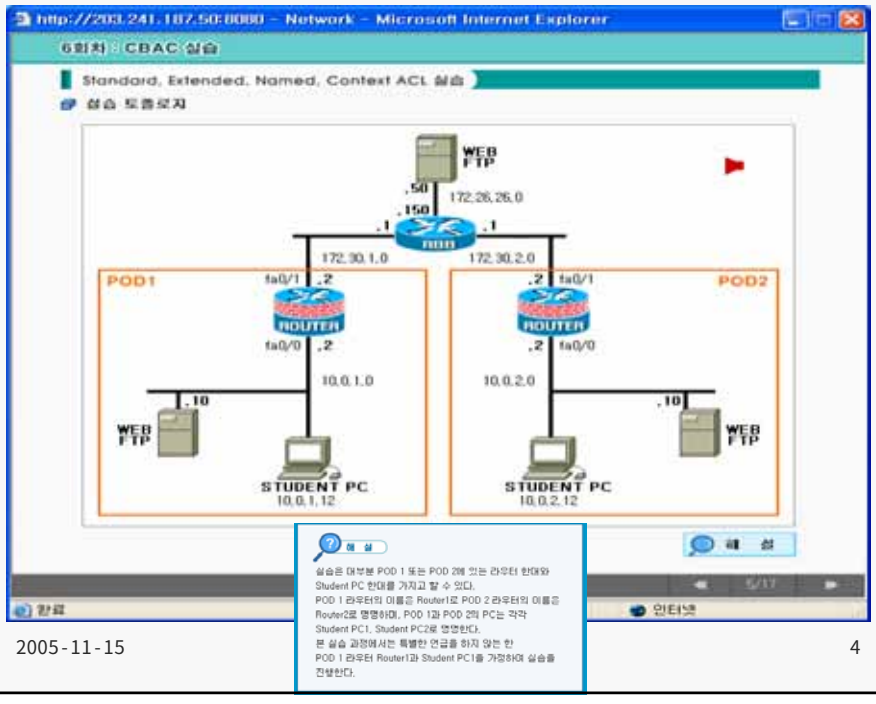
동서대학교/인터넷공학부
이 훈 재
hjlee@dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee
http://crypto.dongseo.ac.kr





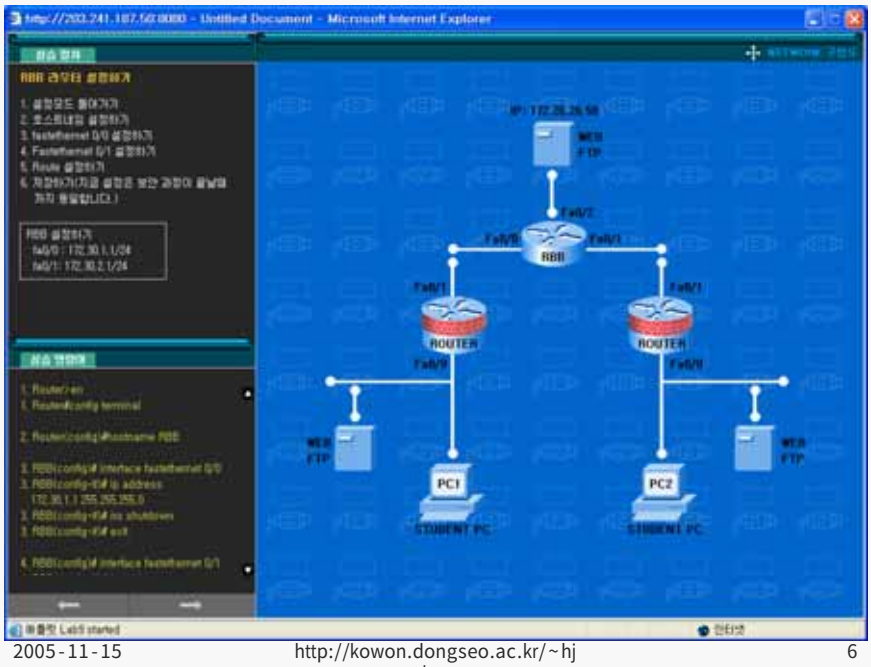

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
6회차 : CBAC 실습
Standard, Extended, Named, Context ACL 실습
목 표
Standard Access List 정의 방법
Extended Access List 정의 방법
Named Access List 정의 방법
Access List 적용 방법
Access List 확인 방법
Access List 에 주석 달기
1/17
완료
인터넷




http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
6회차 : CBAC 실습
Standard, Extended, Named, Context ACL 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
10.0.1.0
10.0.2.0
.10
WEB FTP
STUDENT PC
10.0.1.12
10.0.2.12
해 설
5/17
완료
인터넷

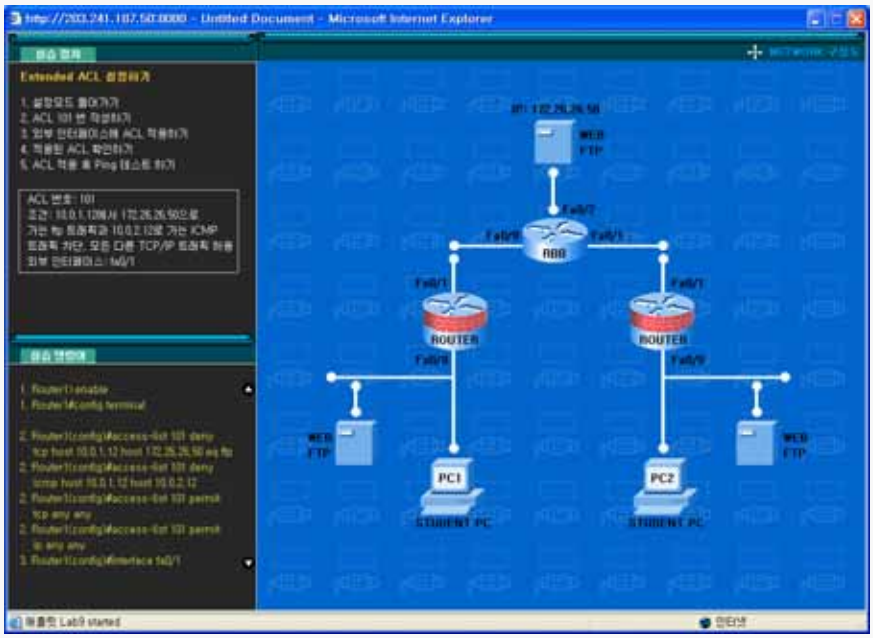

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
6회차 : CBAC 실습
Standard, Extended, Named, Context ACL 실습
실습
제 1 단계 : Standard Access Control List
호스트 10.0.1.12로부터 외부로 나가는 (outbound) 트래픽을 차단하는 standard ACL (ACL number=77)을 작성해본다.
(아래 텍스트 입력란에 access list 77에 대한 syntax를 입력해 보자. ->입력 후 Enter)
Router1(config)#access-list 77 deny 10.0.1.12 0.0.0.0 또는
Router1(config)#access-list 77 deny host 10.0.1.12
인터페이스에 access list를 적용하기 전에 POD 1 내부 호스트 10.0.1.12로부터 POD 2 내부 호스트 10.0.2.12로 Ping 테스트를 수행하여 네트워크 연결성을 확인해 본다.
(ping 테스트는 성공할 것인가?)
위의 standard access list 77을 외부 인터페이스 (outside interface)의 라우터 출력 방향 (outbound) 트래픽에 적용하는 명령어를 입력해 보자. (->입력 후 Enter)
Router1(config)#interface fa0/1
Router1(config-if)#ip access-group 77 out
이제 다시 위의 b에서와 같은 ping 테스트를 해보면 트래픽이 차단되어 ping 테스트에 실패함을 확인할 수 있다.
Standard Access List는 1~99 사이의 ACL 넘버를 사용하며, 시스템 관리자로 하여금 임의의 IP 주소 집합이나 특정 IP 주소로부터의 트래픽을 허용(permit)하거나 거절(deny) 한다.
Ping 테스트는 성공한다. 이는 현재 ACL을 정의하기만 했을 뿐 인터페이스에는 아직 적용하지 않았기 때문에 10.0.1.12 호스트로부터의 네트워크 연결성에는 아무 문제가 없다.
실습하기




http://203.241.187.50:8080 - Untitled Document - Microsoft Internet Explorer
RBB 라우터 설정하기
1. 설정모드 들어가기
2. 호스트네임 설정하기
3. fastethernet 0/0 설정하기
4. Fastethernet 0/1 설정하기
5. Route 설정하기
6. 저장하기(지금 설정한 모든 과정이 물거품 하지 않습니다.)
RBB 설정하기
fa0/0 : 172.30.1.1/24
fa0/1: 172.30.2.1/24
실습 명령어
RBB
ROUTER
ROUTER
PC1
PC2
STUDENT PC
STUDENT PC
Lab3 started
인터넷

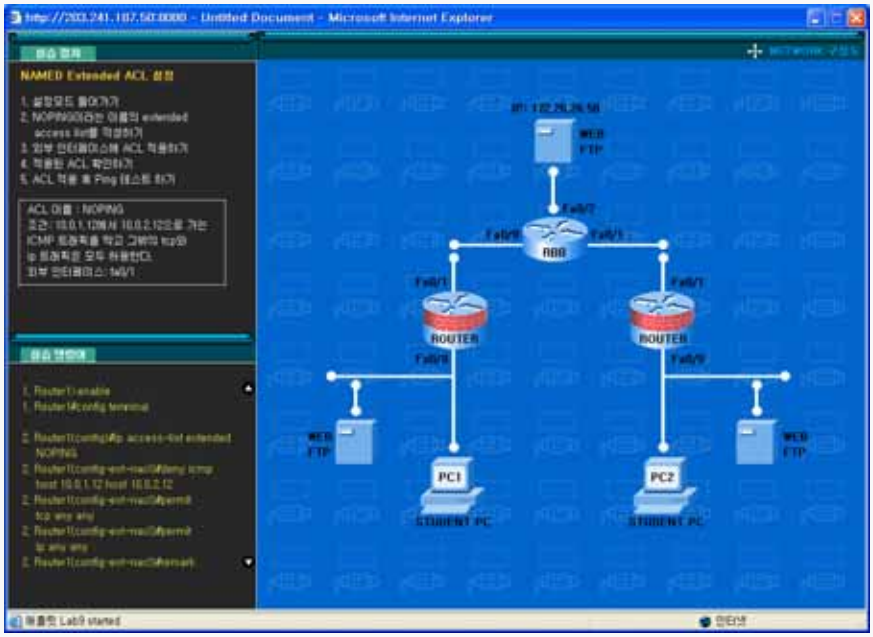

Extended Access List는 시스템 관리자로 하여금 네트워크 트래픽을 훨씬 더 구체적으로 제어할 수 있게 한다. Extended access list는 송신지/수신지 주소 모두를 이용할 수 있으며, 프로토콜이나 포트 번호를 기준으로 트래픽에 대한 필터링도 할 수 있다.





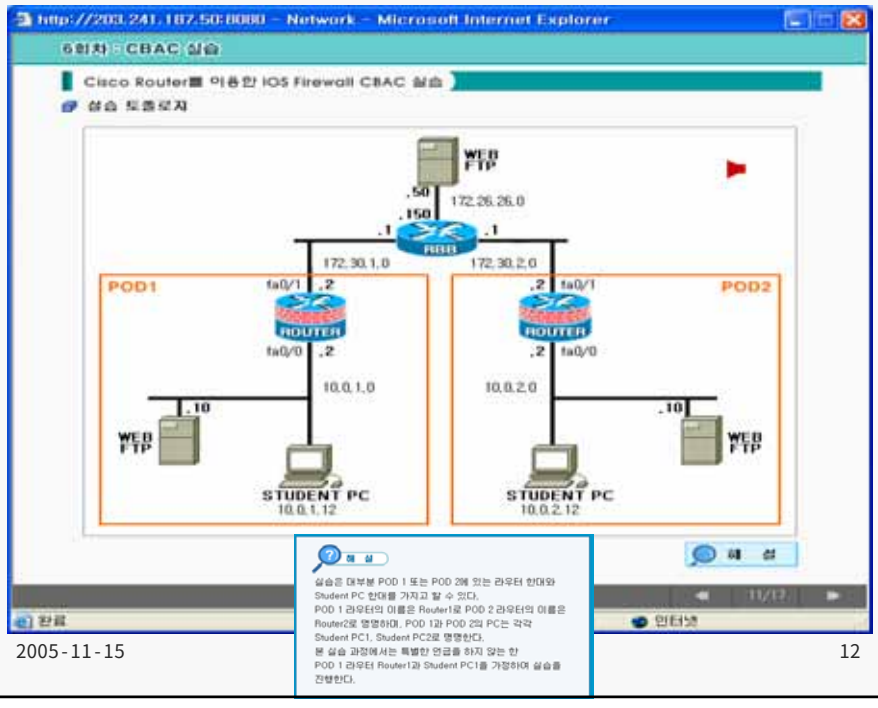

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
6회차 - CBAC 실습
Standard, Extended, Named, Context ACL 실습
실습
제 3 단계: Named IP Access Control List
NOPING이라는 이름의 extended access list를 작성해 보자.(※입력 후 Enter)
Router1(config)#ip access-list extended NOPING
아래와 같은 파라미터를 갖는 extended named ACL을 작성해 보자.(※입력 후 Enter)
- 호스트 10.0.1.12에서 호스트 10.0.2.12로의 icmp 트래픽 차단
- 모든 다른 TCP 트래픽 허용
- 모든 다른 IP 트래픽 허용
Router1(config-ext-nacl)#deny icmp host 10.0.1.12 host 10.0.2.12
Router1(config-ext-nacl)#permit tcp any any
Router1(config-ext-nacl)#permit ip any any
라우터에의 named ACL 적용과 적용된 named ACL의 확인 방법은 이전과 동일하다.
제 4 단계: Access List에 주석 달기
ACL에 주석을 달기 위해서는 remark 명령어를 사용한다.
(예) Router1(config-ext-nacl)#remark NOPING is a named ACL.
running configuration을 보면 ACL에 대한 주석을 볼 수 있다.
(예) Router1#show running-config
실습하기
완료
인터넷
Standard Access List와 Extended Access List에는 이름을 붙일 수 있다. Access List를 명명하는 명령어는 아래와 같다. 단, global configuration mode에서 입력해야 한다.
ip access-list {standard|extended} name




http://203.241.187.50:8080 - Untitled Document - Microsoft Internet Explorer
NAMED Extended ACL 실습
ACL 이름 : NOPING
ROUTER
ROUTER
PC1
PC2
STUDENT PC
STUDENT PC


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
6회차 - CBAC 실습
Cisco Router를 이용한 IOS Firewall CBAC 실습
목 표
Logging과 Audit Trails 설정
ACL (Access Control List)에 대한 검사 규칙 정의 및 적용
CBAC (Context-based Access Control) 테스트 및 확인
완료
인터넷




http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
6회차 - CBAC 실습
Cisco Router를 이용한 IOS Firewall CBAC 실습
실습 토폴로지
WEB FTP
.50
172.26.26.0
.150
.1
.1
RRR
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
10.0.2.12
해 설
실습은 대부분 POD 1 또는 POD 2에 있는 라우터 한대와
Student PC 한대를 가지고 할 수 있다.
POD 1 라우터의 이름은 Router1로 POD 2 라우터의 이름은
Router2로 명명하며, POD 1과 POD 2의 PC는 각각
Student PC1, Student PC2로 명명한다.
본 실습 과정에서는 특별한 언급을 하지 않는 한
POD 1 라우터 Router1과 Student PC1을 가정하여 실습을
진행한다.
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
6회차 - CBAC 실습
Cisco Router를 이용한 IOS Firewall CBAC 실습
실습
제 1 단계: Logging과 Audit Trails 설정
Console과 Syslog server로의 logging을 enable 한다.
(단, syslog server는 호스트 10.0.1.12에 설정되어 있다고 한다.) (※입력 후 Enter)
Router1(config)#logging on
Router1(config)#loggin 10.0.1.12
다음으로 audit trail을 enable 한다.(※입력 후 Enter)
Router1(config)#ip inspect audit-trail
구체적인 logging 정보를 보기 위해서는 show logging 명령어를 사용할 수 있으며,
logging buffer 내의 항목들을 지우기 위해서는 clear logging 명령어를 사용한다.
(예) Router1#show logging
(예) Router1#clear logging
12/17
완료
인터넷

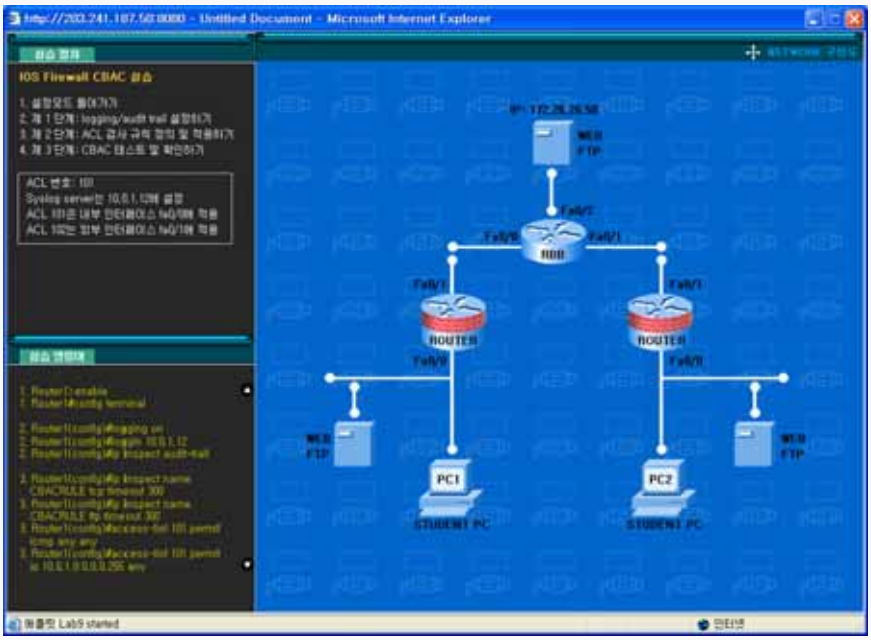



http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
6회차 - CBAC 실습
Cisco Router를 이용한 IOS Firewall CBAC 실습
실습
제 2 단계: ACL에 대한 검사 규칙 정의 및 적용
모든 TCP 및 FTP 트래픽을 검사하기 위한 CBAC 규칙을 정의한다.
단, 검사 규칙명은 CBAC으로 하고 timeout은 5분으로 한다.(※입력 후 Enter)
Router1(config)#ip inspect name CBACRULE tcp timeout 300
Router1(config)#ip inspect name CBACRULE ftp timeout 300
Outbound ICMP 트래픽과 CBAC 트래픽을 허용하는 ACL을 정의하고, 그 외의 내부에서
발생하는 모든 다른 트래픽은 차단한다. ACL 번호는 101번을 사용한다.(※입력 후 Enter)
Router1(config)#access-list 101 permit icmp any any
Router1(config)#access-list 101 permit ip 10.0.1.0 0.0.0.255 any
Router1(config)#access-list 101 deny ip any any
Inbound ICMP 트래픽을 허용하는 ACL을 정의하고, 그 외의 외부에서 발생한 다른 모든
트래픽은 차단한다. ACL 번호는 102번을 사용한다.(※입력 후 Enter)
Router1(config)#access-list 102 permit icmp any any
13/17
완료
인터넷

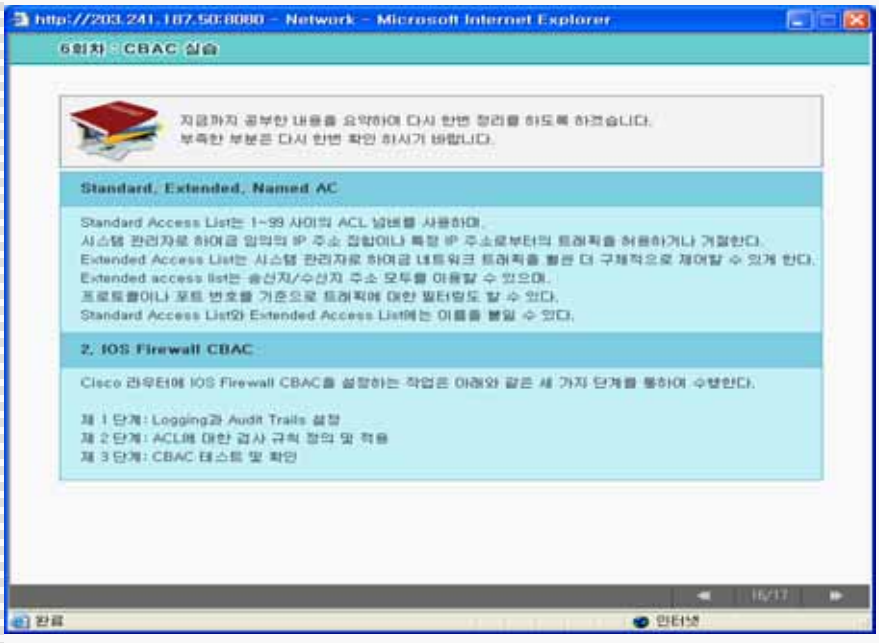

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
6회차 : CBAC 실습
Cisco Router를 이용한 IOS Firewall CBAC 실습
실습
제 2 단계 : ACL에 대한 검사 규칙 정의 및 적용
검사 규칙과 ACL 101을 내부 인터페이스 (fa0/0)에 적용한다. (↵입력 후 Enter)
Router1(config)#interface fa0/0
Router1(config-if)#ip inspect CBACRULE in
Router1(config-if)#ip access-group 101 in
ACL 102를 외부 인터페이스 (fa0/1)에 적용한다.(↵입력 후 Enter)
Router1(config)#interface fa0/1
Router1(config-if)#ip access-group 102 in
14/17
완료
인터넷




http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
6회차 : CBAC 실습
Cisco Router를 이용한 IOS Firewall CBAC 실습
실습
제 3 단계 : CBAC 테스트 및 확인
CBAC 설정을 확인하는 명령어를 입력해 본다 (총 3 개 명령어). (↵입력 후 Enter)
Router1(config)#interface fa0/0
Router1(config-if)#ip inspect CBACRULE in
Router1(config-if)#ip access-group 101 in
CBAC 설정을 확인하는 명령어를 입력해 본다 (총 3 개 명령어). (↵입력 후 Enter)
Router1#show ip inspect sessions
Router1#show ip inspect sessions detail
Router1#show ip inspect all
실습하기
15/17
완료
인터넷


http://203.241.187.50:8080 - Untitled Document - Microsoft Internet Explorer
IOS Firewall CBAC 실습
ROUTER
ROUTER
PC1
PC2
STUDENT PC
STUDENT PC




http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
6회차 : CBAC 실습
Standard, Extended, Named AC
2. IOS Firewall CBAC

# End of Lecture