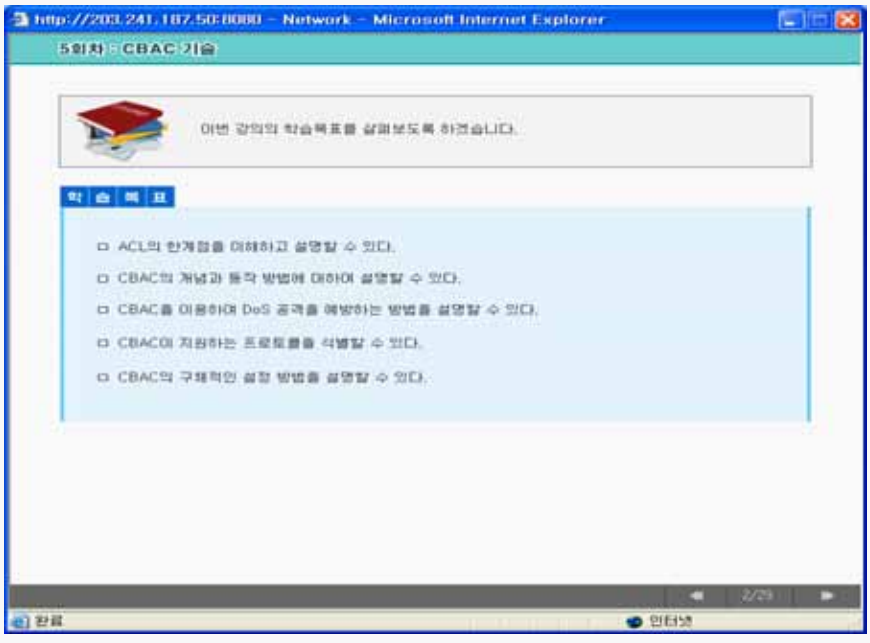
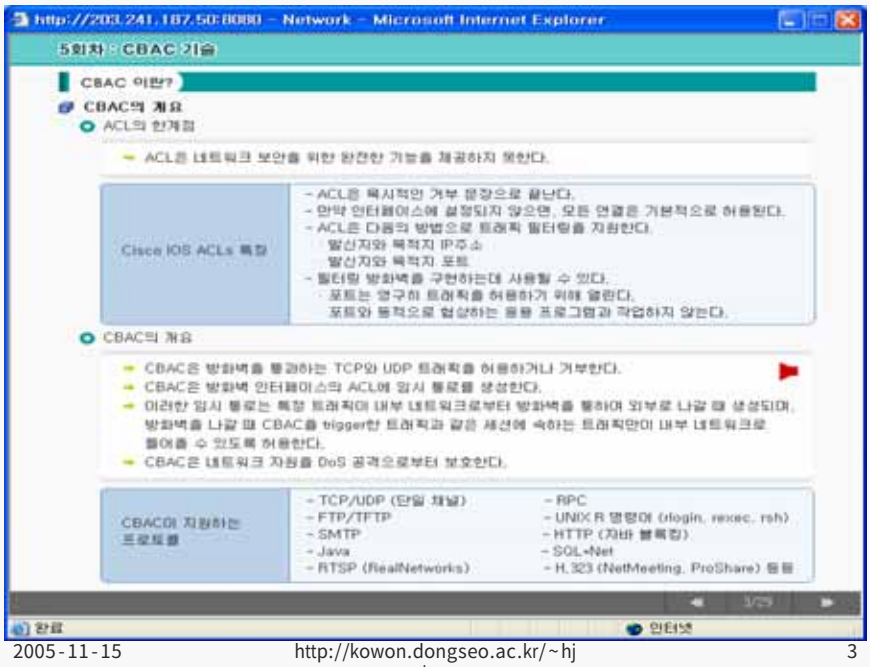
FNS

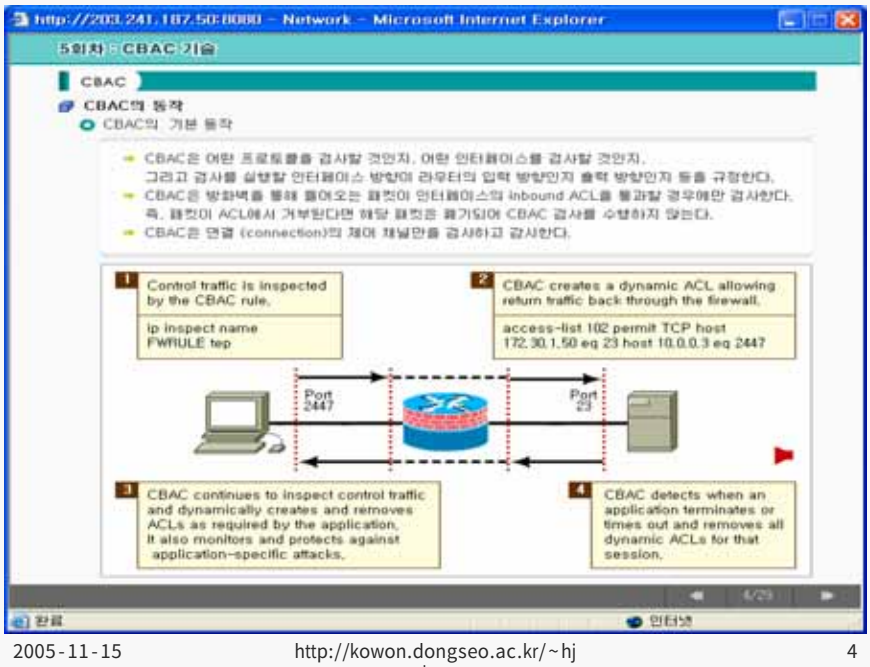
(Fundamental Network Security)

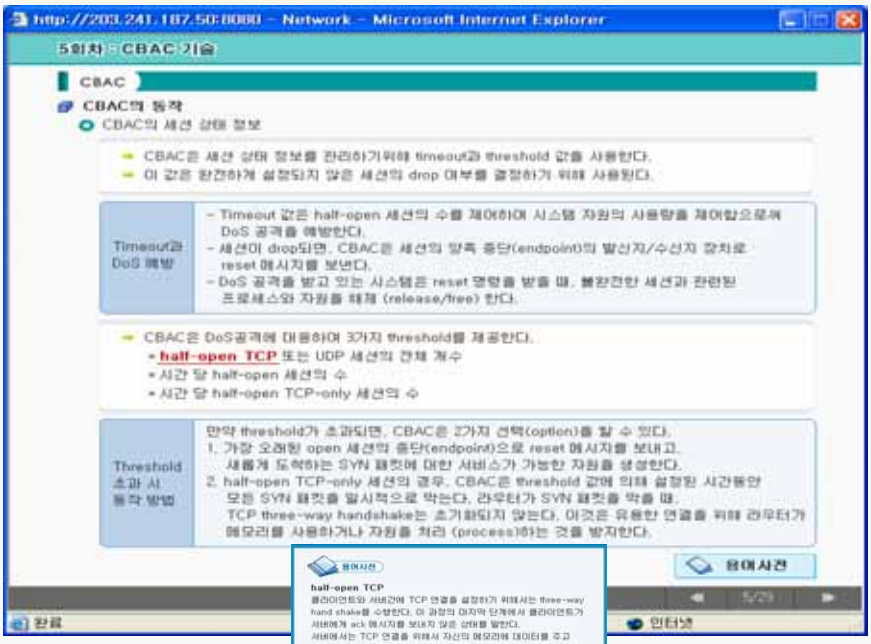
Ch5. CBAC(Context-based Access Control) 기술

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

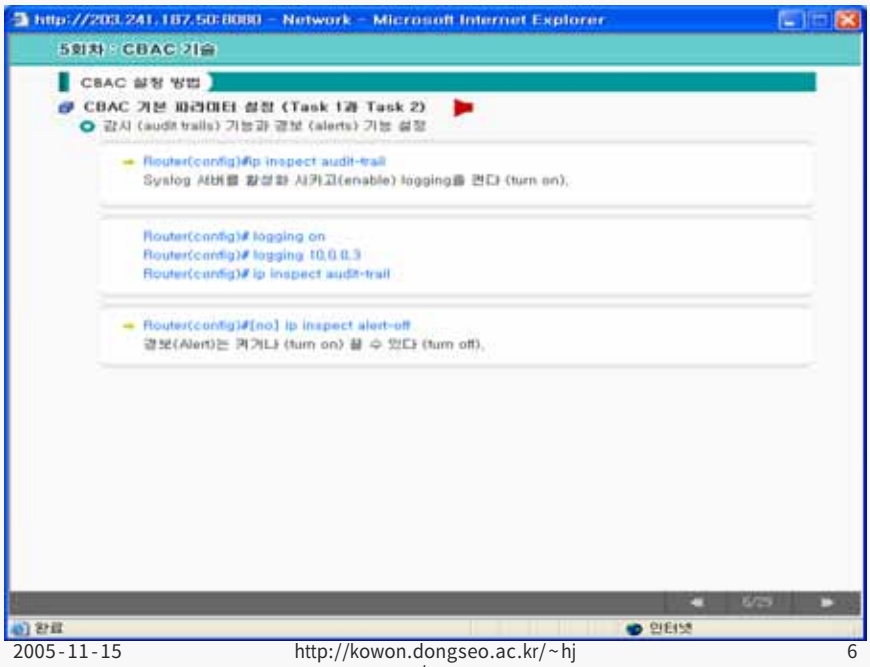



http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 : CBAC 기술
CBAC 이란?
CBAC의 개요
ACL의 한계점
ACL은 네트워크 보안을 위한 완전한 기능을 제공하지 못한다.
Cisco IOS ACLs 특징
- ACL은 묵시적인 거부 문장으로 끝난다.
- 만약 인터페이스에 설정되지 않으면, 모든 연결은 기본적으로 허용된다.
- ACL은 다음의 방법으로 트래픽 필터링을 지원한다.
발신지와 목적지 IP주소
발신지와 목적지 포트
- 필터링 방화벽을 구현하는데 사용될 수 있다.
포트는 영구히 트래픽을 허용하기 위해 열린다.
포트와 동적으로 협상하는 응용 프로그램과 작업하지 않는다.
CBAC의 개요
CBAC은 방화벽을 통과하는 TCP와 UDP 트래픽을 허용하거나 거부한다.
CBAC은 방화벽 인터페이스의 ACL에 임시 통로를 생성한다.
이러한 임시 통로는 특정 트래픽이 내부 네트워크로부터 방화벽을 통하여 외부로 나갈 때 생성되며, 방화벽을 나갈 때 CBAC을 trigger한 트래픽과 같은 세션에 속하는 트래픽만이 내부 네트워크로 들어올 수 있도록 허용한다.
CBAC은 네트워크 자원을 DoS 공격으로부터 보호한다.
CBAC이 지원하는 프로토콜
- TCP/UDP (단일 채널)
- FTP/TFTP
- SMTP
- Java
- RTSP (RealNetworks)
- RPC
- UNIX R 명령어 (rlogin, rexec, rsh)
- HTTP (자바 블록킹)
- SQL*Net
- H.323 (NetMeeting, ProShare) 등등
1/29
완료
인터넷

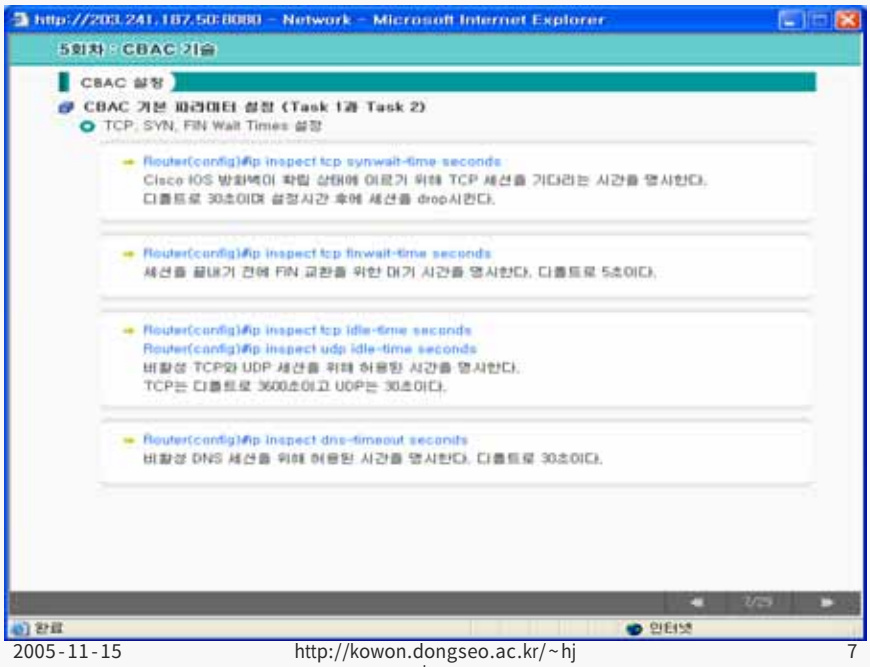

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 : CBAC 기술
CBAC
CBAC의 동작
CBAC의 기본 동작
CBAC은 어떤 프로토콜을 검사할 것인지, 어떤 인터페이스를 검사할 것인지,
그리고 검사를 실행할 인터페이스 방향이 라우터의 입력 방향인지 출력 방향인지 등을 규정한다.
CBAC은 방화벽을 통해 들어오는 패킷이 인터페이스의 inbound ACL을 통과할 경우에만 검사한다.
즉, 패킷이 ACL에서 거부된다면 해당 패킷은 폐기되며 CBAC 검사를 수행하지 않는다.
CBAC은 연결 (connection)의 제어 채널만을 검사하고 감시한다.
1 Control traffic is inspected by the CBAC rule.
ip inspect name FWRULE tcp
2 CBAC creates a dynamic ACL allowing return traffic back through the firewall.
access-list 102 permit TCP host 172.30.1.50 eq 23 host 10.0.0.3 eq 2447
Port 2447
Port 23
3 CBAC continues to inspect control traffic and dynamically creates and removes ACLs as required by the application. It also monitors and protects against application-specific attacks.
4 CBAC detects when an application terminates or times out and removes all dynamic ACLs for that session.
6/29
완료
인터넷



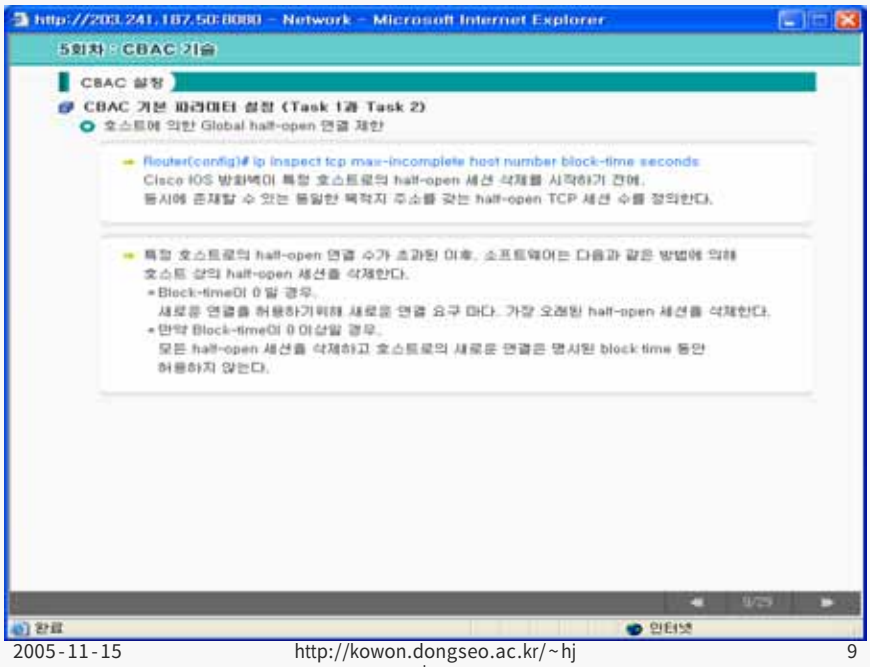
2005-11-15 5

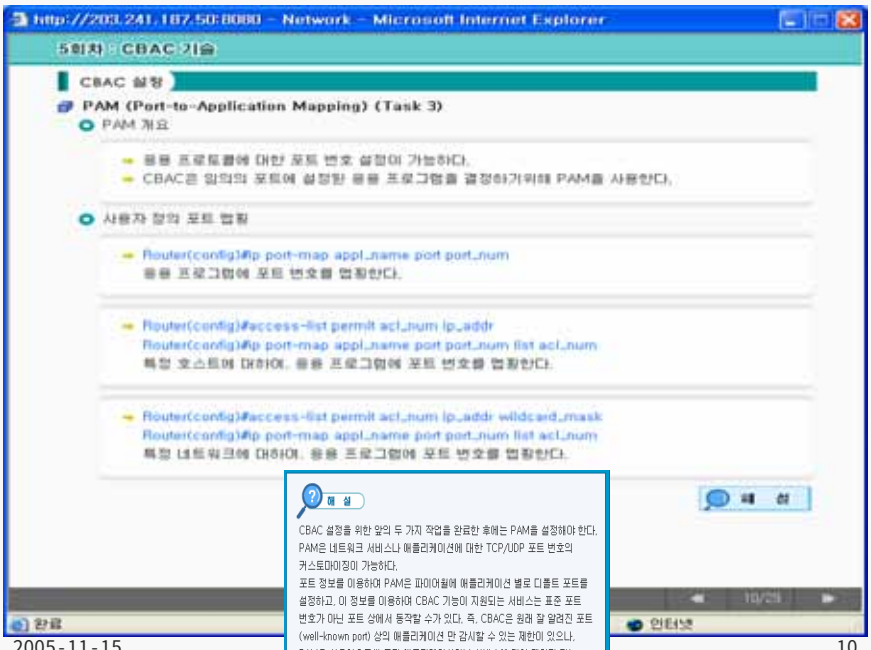


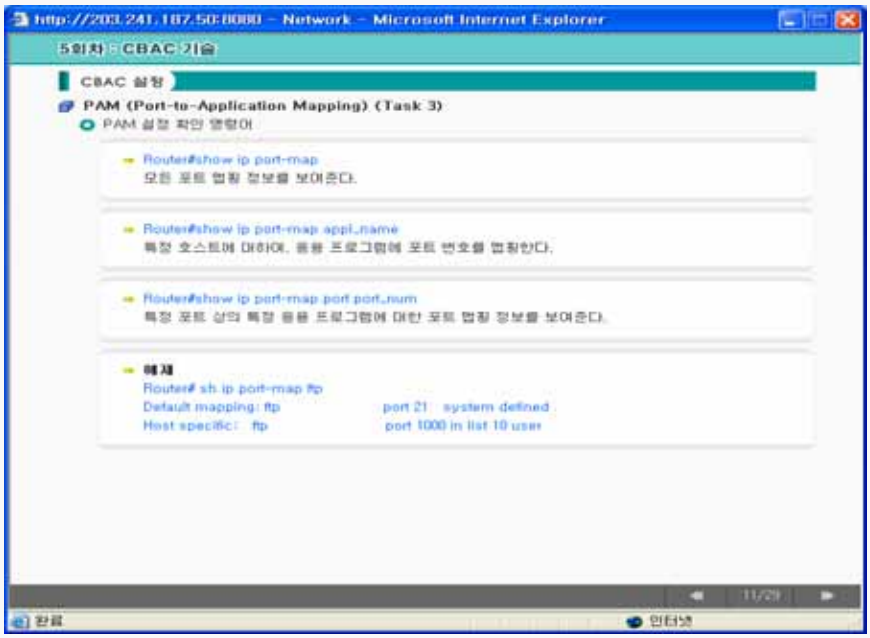
2005-11-15 http://kowon.dongseo.ac.kr/~hjlee 6

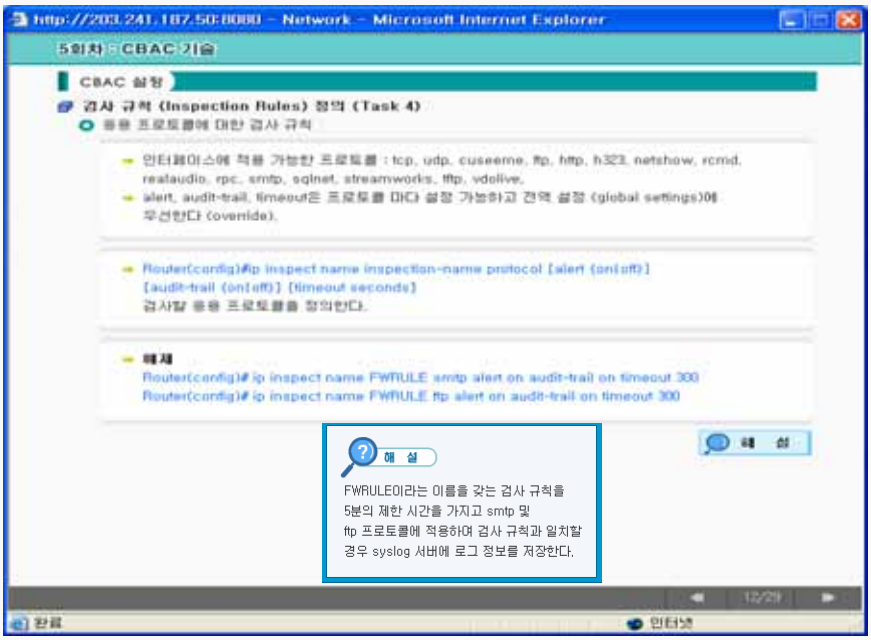

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 : CBAC 기술
CBAC 설정
CBAC 기본 파라메터 설정 (Task 1과 Task 2)
TCP, SYN, FIN Wait Times 설정
Router(config)#ip inspect tcp synwait-time seconds
Cisco IOS 방화벽이 확립 상태에 이르기 위해 TCP 세션을 기다리는 시간을 명시한다.
디폴트로 30초이며 설정시간 후에 세션을 drop시킨다.
Router(config)#ip inspect tcp finwait-time seconds
세션을 끝내기 전에 FIN 교환을 위한 대기 시간을 명시한다. 디폴트로 5초이다.
Router(config)#ip inspect tcp idle-time seconds
Router(config)#ip inspect udp idle-time seconds
비활성 TCP와 UDP 세션을 위해 허용된 시간을 명시한다.
TCP는 디폴트로 3600초이고 UDP는 30초이다.
Router(config)#ip inspect dns-timeout seconds
비활성 DNS 세션을 위해 허용된 시간을 명시한다. 디폴트로 30초이다.
1/29
완료
인터넷

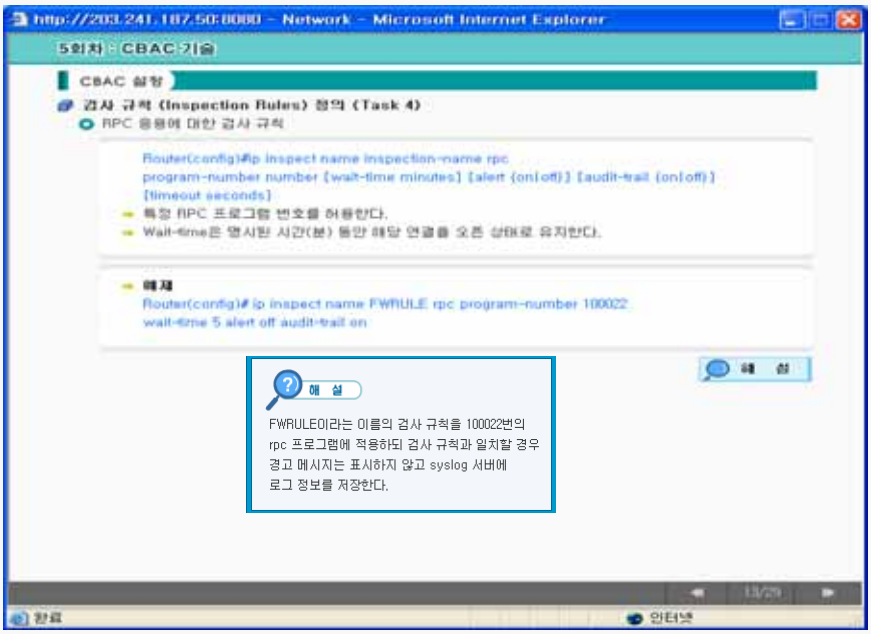

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 : CBAC 기술
CBAC 설정
CBAC 기본 파라메터 설정 (Task 1과 Task 2)
Global half-open 연결 제한
Router(config)#ip inspect max-incomplete high number
소프트웨어가 half-open 세션 삭제를 시작하는 half-open 세션 수를 정의한다.(aggressive mode)
디폴트 값은 500임.
Router(config)#ip inspect max-incomplete low number
소프트웨어가 half-open 세션 삭제를 멈추는 half-open 세션 수를 정의한다.
디폴트 값은 400임.
Router(config)#ip inspect one-minute high number
1 분당 새로운 half-open 세션 수를 정의하며, 이 수 이상의 세션이 발생할 경우
그 때부터의 세션은 삭제된다.
Router(config)#ip inspect one-minute low number
1 분당 새로운 half-open 세션 수를 정의하며, 이 수 이하의 세션이 발생할 경우
세션 삭제는 종료된다.
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 : CBAC 기술
CBAC 설정
CBAC 기본 파라메터 설정 (Task 1과 Task 2)
호스트에 의한 Global half-open 연결 제한
Router(config)# ip inspect tcp max-incomplete host number block-time seconds
Cisco IOS 방화벽이 특정 호스트로의 half-open 세션 삭제를 시작하기 전에,
동시에 존재할 수 있는 동일한 목적지 주소를 갖는 half-open TCP 세션 수를 정의한다.
특정 호스트로의 half-open 연결 수가 초과된 이후, 소프트웨어는 다음과 같은 방법에 의해
호스트 상의 half-open 세션을 삭제한다.
• Block-time이 0 일 경우,
새로운 연결을 허용하기위해 새로운 연결 요구 마다, 가장 오래된 half-open 세션을 삭제한다.
• 만약 Block-time이 0 이상일 경우,
모든 half-open 세션을 삭제하고 호스트로의 새로운 연결은 명시된 block time 동안
허용하지 않는다.
9/29
완료
인터넷

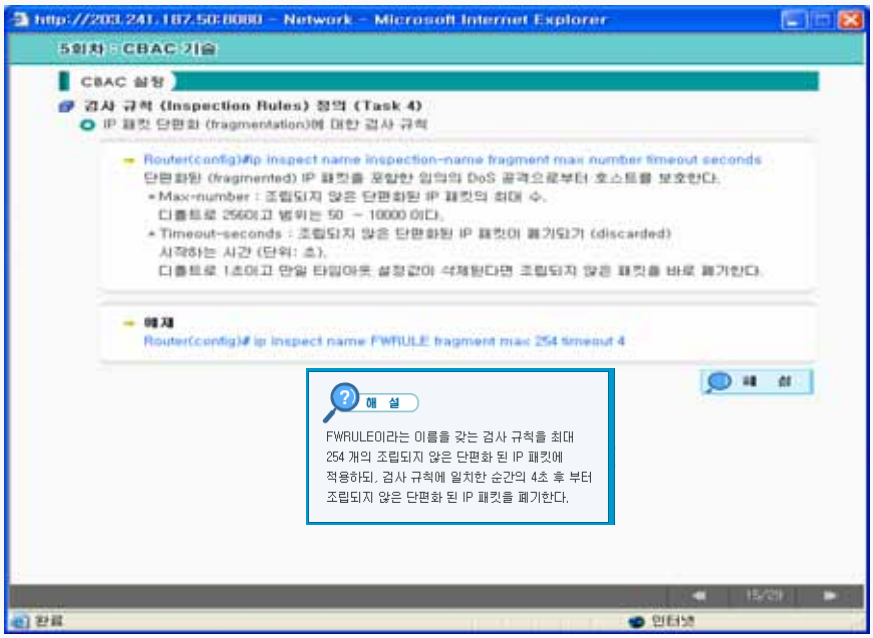

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 : CBAC 기술
CBAC 설정
PAM (Port-to-Application Mapping) (Task 3)
PAM 개요
응용 프로토콜에 대한 포트 번호 설정이 가능하다.
CBAC은 임의의 포트에 설정된 응용 프로그램을 결정하기위해 PAM을 사용한다.
사용자 정의 포트 맵핑
Router(config)#ip port-map appl_name port port_num
응용 프로그램에 포트 번호를 맵핑한다.
Router(config)#access-list permit acl_num ip_addr
Router(config)#ip port-map appl_name port port_num list acl_num
특정 호스트에 대하여, 응용 프로그램에 포트 번호를 맵핑한다.
Router(config)#access-list permit acl_num ip_addr wildcard_mask
Router(config)#ip port-map appl_name port port_num list acl_num
특정 네트워크에 대하여, 응용 프로그램에 포트 번호를 맵핑한다.
해 설
CBAC 설정을 위한 앞의 두 가지 작업을 완료한 후에는 PAM을 설정해야 한다.
PAM은 네트워크 서비스나 애플리케이션에 대한 TCP/UDP 포트 번호의
커스토마이징이 가능하다.
포트 정보를 이용하여 PAM은 파이어월에 애플리케이션 별로 디폴트 포트를
설정하고, 이 정보를 이용하여 CBAC 기능이 지원되는 서비스는 표준 포트
번호가 아닌 포트 상에서 동작할 수가 있다. 즉, CBAC은 원래 잘 알려진 포트
(well-known port) 상의 애플리케이션 만 감시할 수 있는 제한이 있으나,
PAM을 사용함으로써 특정 애플리케이션이나 서비스에 대한 제어가 가능
하지는 특징을 가지게 된다.
10/29
완료
인터넷

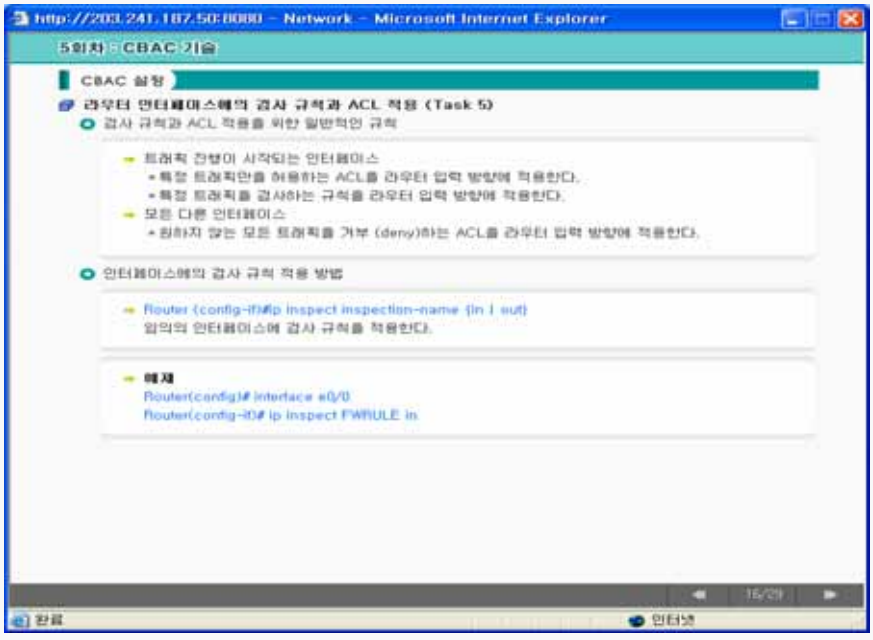

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 : CBAC 기술
CBAC 설정
PAM (Port-to-Application Mapping) (Task 3)
PAM 설정 확인 명령어
Router#show ip port-map
모든 포트 맵핑 정보를 보여준다.
Router#show ip port-map appl_name
특정 호스트에 대하여, 응용 프로그램에 포트 번호를 맵핑한다.
Router#show ip port-map port port_num
특정 포트 상의 특정 응용 프로그램에 대한 포트 맵핑 정보를 보여준다.
예제
Router# sh ip port-map ftp
Default mapping: ftp port 21 system defined
Host specific: ftp port 1000 in list 10 user
11/29
완료
인터넷

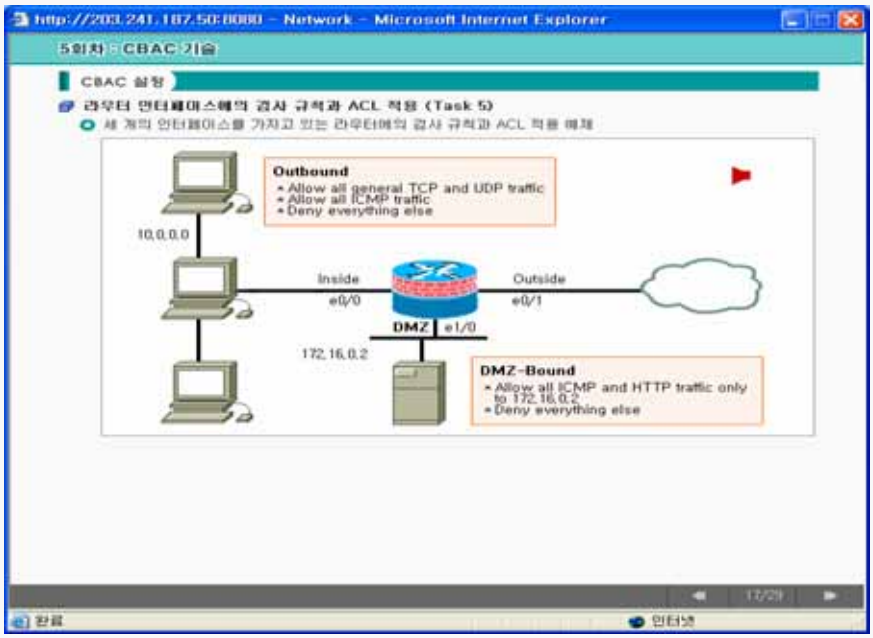

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 : CBAC 기술
CBAC 설정
검사 규칙 (Inspection Rules) 정의 (Task 4)
응용 프로토콜에 대한 검사 규칙
인터페이스에 적용 가능한 프로토콜 : tcp, udp, cuseeme, ftp, http, h323, netshow, rcmd, realaudio, rpc, smtp, sqlnet, streamworks, tftp, vdolive,
alert, audit-trail, timeout은 프로토콜 마다 설정 가능하고 전역 설정 (global settings)에 우선한다 (override).
Router(config)#ip inspect name inspection-name protocol [alert (on|off)] [audit-trail (on|off)] [timeout seconds]
검사할 응용 프로토콜을 정의한다.
예제
Router(config)# ip inspect name FWRULE smtp alert on audit-trail on timeout 300
Router(config)# ip inspect name FWRULE ftp alert on audit-trail on timeout 300
해 설
FWRULE이라는 이름을 갖는 검사 규칙을 5분의 제한 시간을 가지고 smtp 및 ftp 프로토콜에 적용하여 검사 규칙과 일치할 경우 syslog 서버에 로그 정보를 저장한다.
12/29
완료
인터넷

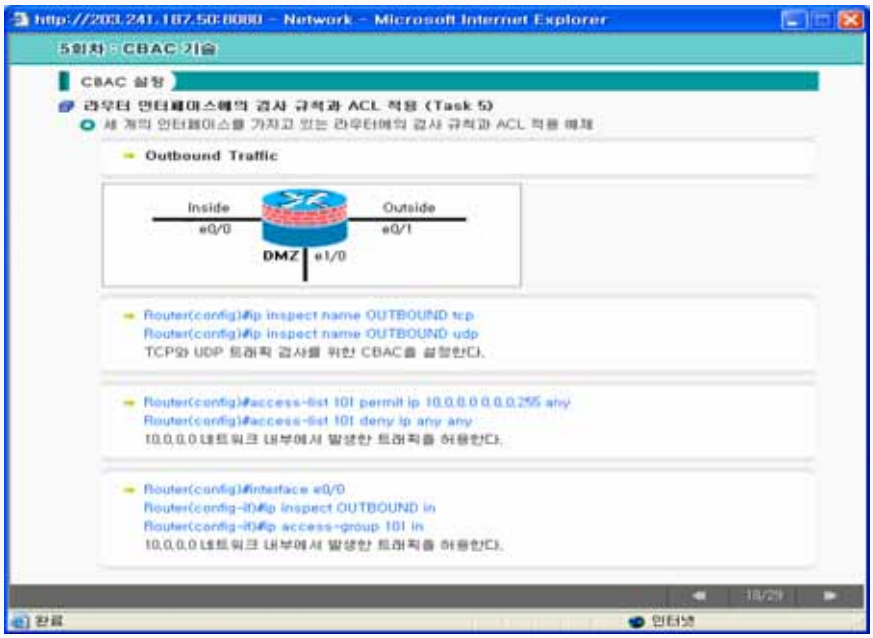

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 - CBAC 기술
CBAC 설정
검사 규칙 (Inspection Rules) 정의 (Task 4)
RPC 응용에 대한 검사 규칙
Router(config)#ip inspect name inspection-name rpc
program-number number [wait-time minutes] [alert {on|off}] [audit-trail {on|off}]
[timeout seconds]
특정 RPC 프로그램 번호를 허용한다.
Wait-time은 명시된 시간(분) 동안 해당 연결을 오픈 상태로 유지한다.
예제
Router(config)# ip inspect name FWRULE rpc program-number 100022
wait-time 5 alert off audit-trail on
해 설
해 설
FWRULE이라는 이름의 검사 규칙을 100022번의
rpc 프로그램에 적용하되 검사 규칙과 일치할 경우
경고 메시지는 표시하지 않고 syslog 서버에
로그 정보를 저장한다.
13/29
완료
인터넷

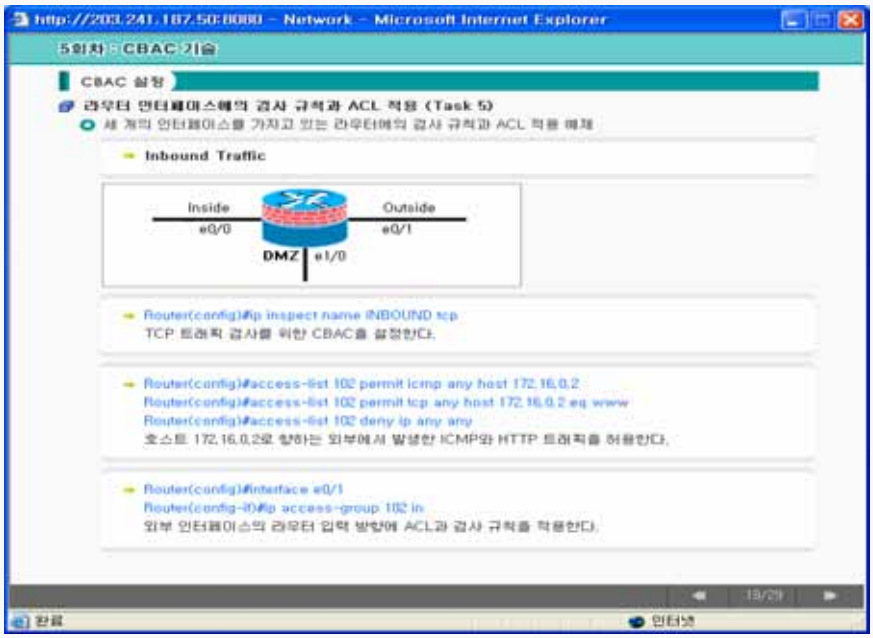

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 - CBAC 기술
CBAC 설정
검사 규칙 (Inspection Rules) 정의 (Task 4)
SMTP 응용에 대한 검사 규칙
Router(config)#ip inspect name inspection-name smtp [alert {on|off}] [audit-trail {on|off}]
[timeout seconds]
SMTP 응용에서 다음과 같은 합법적인 명령어만을 허용한다.
*DATA, EXPN, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML, VRFY,
이 기능이 disable 되어 있으면, 모든 SMTP 명령어가 방화벽을 통과할 수 있게 되고,
이는 잠재적인 메일 서버 취약점 노출로 이어진다.
예제
Router(config)# ip inspect name FWRULE smtp
해 설
해 설
FWRULE이라는 이름을 갖는 검사 규칙을
smtp 프로토콜에 적용한다.
14/29
완료
인터넷

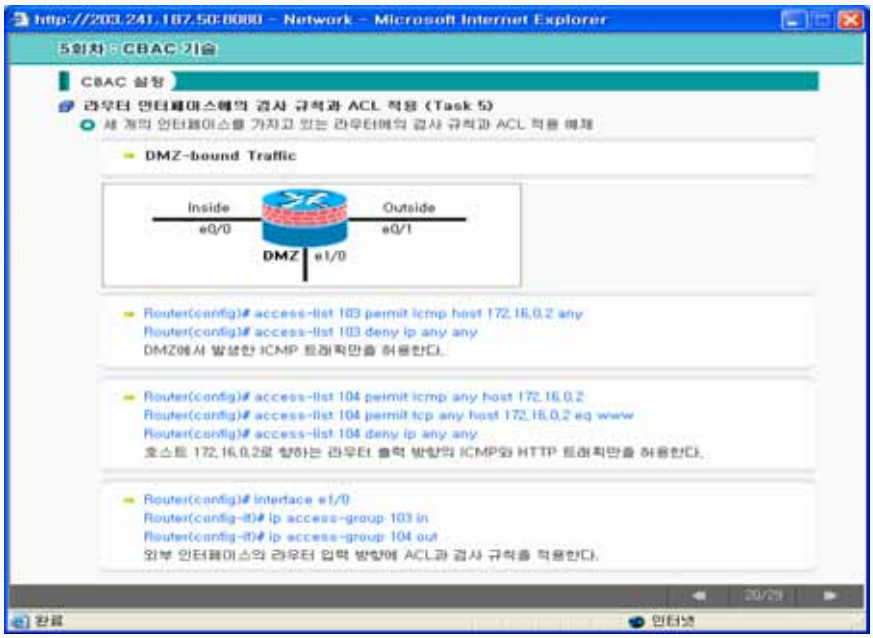

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 CBAC 2/2
CBAC 설정
검사 규칙 (Inspection Rules) 정의 (Task 4)
IP 패킷 단편화 (fragmentation)에 대한 검사 규칙
Router(config)#ip inspect name inspection-name fragment max number timeout seconds
단편화된 (fragmented) IP 패킷을 포함한 임의의 DoS 공격으로부터 호스트를 보호한다.
• Max-number : 조립되지 않은 단편화된 IP 패킷의 최대 수.
디폴트로 256이고 범위는 50 ~ 10000 이다.
• Timeout-seconds : 조립되지 않은 단편화된 IP 패킷이 폐기되기 (discarded)
시작하는 시간 (단위: 초).
디폴트로 1초이고 만일 타임아웃 설정값이 삭제된다면 조립되지 않은 패킷을 바로 폐기한다.
예제
Router(config)# ip inspect name FWRULE fragment max 254 timeout 4
해 설
해 설
FWRULE이라는 이름을 갖는 검사 규칙을 최대 254 개의 조립되지 않은 단편화 된 IP 패킷에 적용하되, 검사 규칙에 일치한 순간의 4초 후 부터 조립되지 않은 단편화 된 IP 패킷을 폐기한다.
15/29
완료
인터넷

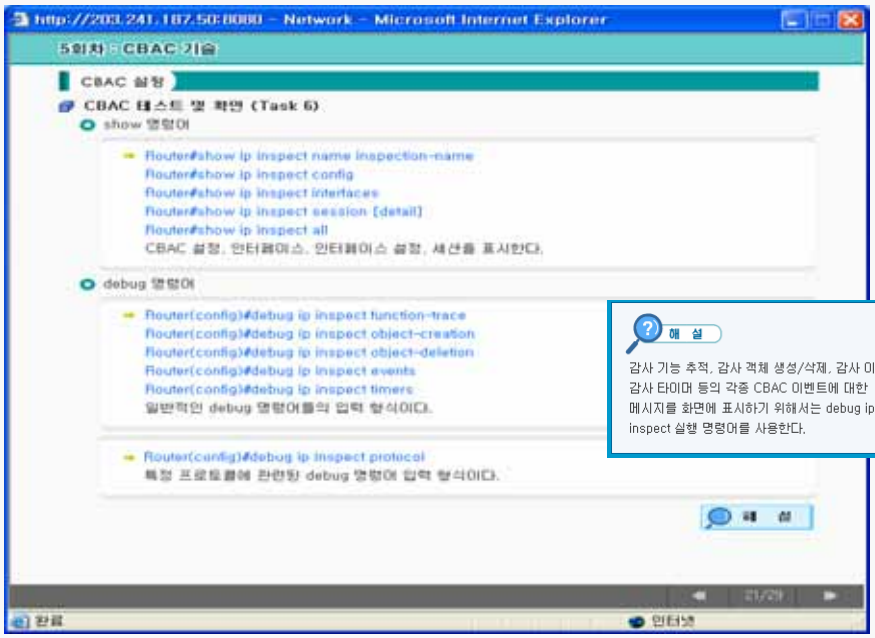

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 CBAC 2/2
CBAC 설정
라우터 인터페이스에의 검사 규칙과 ACL 적용 (Task 5)
검사 규칙과 ACL 적용을 위한 일반적인 규칙
트래픽 진행이 시작되는 인터페이스
• 특정 트래픽만을 허용하는 ACL을 라우터 입력 방향에 적용한다.
• 특정 트래픽을 검사하는 규칙을 라우터 입력 방향에 적용한다.
모든 다른 인터페이스
• 원하지 않는 모든 트래픽을 거부 (deny)하는 ACL을 라우터 입력 방향에 적용한다.
인터페이스에의 검사 규칙 적용 방법
Router (config-if)#ip inspect inspection-name {in | out}
임의의 인터페이스에 검사 규칙을 적용한다.
예제
Router(config)# interface e0/0
Router(config-if)# ip inspect FWRULE in
16/29
완료
인터넷

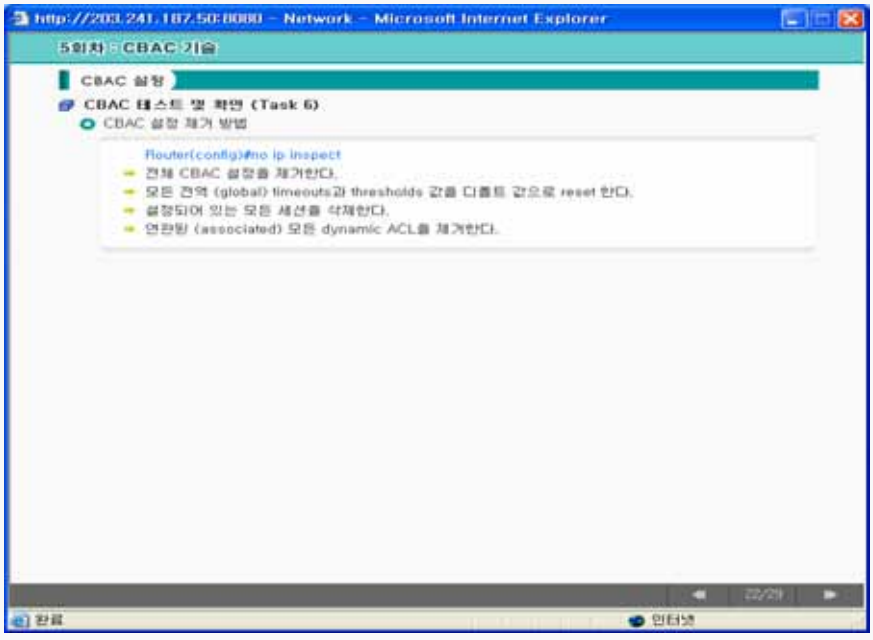

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 CBAC 기술
CBAC 설정
라우터 인터페이스에의 검사 규칙과 ACL 적용 (Task 5)
세 개의 인터페이스를 가지고 있는 라우터에의 검사 규칙과 ACL 적용 예제
Outbound
* Allow all general TCP and UDP traffic
* Allow all ICMP traffic
* Deny everything else
10.0.0.0
Inside
e0/0
Outside
e0/1
DMZ
e1/0
172.16.0.2
DMZ-Bound
* Allow all ICMP and HTTP traffic only to 172.16.0.2
* Deny everything else
17/29
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 CBAC 기술
CBAC 설정
라우터 인터페이스에의 검사 규칙과 ACL 적용 (Task 5)
세 개의 인터페이스를 가지고 있는 라우터에의 검사 규칙과 ACL 적용 예제
Outbound Traffic
Inside
e0/0
Outside
e0/1
DMZ
e1/0
Router(config)#ip inspect name OUTBOUND tcp
Router(config)#ip inspect name OUTBOUND udp
TCP와 UDP 트래픽 검사를 위한 CBAC를 설정한다.
Router(config)#access-list 101 permit ip 10.0.0.0 0.0.0.255 any
Router(config)#access-list 101 deny ip any any
10.0.0.0 네트워크 내부에서 발생한 트래픽을 허용한다.
Router(config)#interface e0/0
Router(config-if)#ip inspect OUTBOUND in
Router(config-if)#ip access-group 101 in
10.0.0.0 네트워크 내부에서 발생한 트래픽을 허용한다.
18/29
완료
인터넷

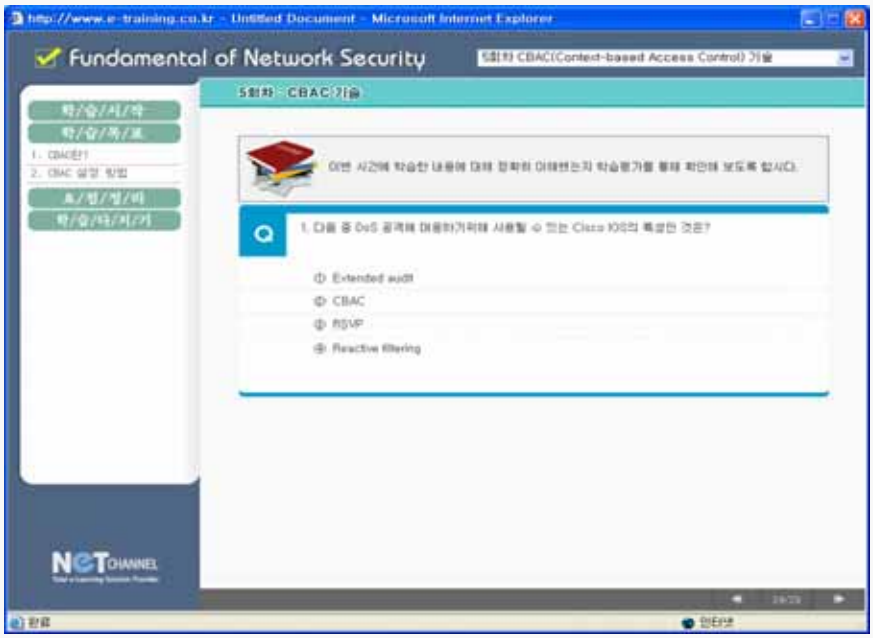

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 CBAC 2/3
CBAC 설정
라우터 인터페이스에의 검사 규칙과 ACL 적용 (Task 5)
세 개의 인터페이스를 가지고 있는 라우터에의 검사 규칙과 ACL 적용 예제
Inbound Traffic
Inside
e0/0
Outside
e0/1
DMZ
e1/0
Router(config)#ip inspect name INBOUND tcp
TCP 트래픽 검사를 위한 CBAC를 설정한다.
Router(config)#access-list 102 permit icmp any host 172.16.0.2
Router(config)#access-list 102 permit tcp any host 172.16.0.2 eq www
Router(config)#access-list 102 deny ip any any
호스트 172.16.0.2로 향하는 외부에서 발생한 ICMP와 HTTP 트래픽을 허용한다.
Router(config)#interface e0/1
Router(config-if)#ip access-group 102 in
외부 인터페이스의 라우터 입력 방향에 ACL과 검사 규칙을 적용한다.
19/29
완료
인터넷

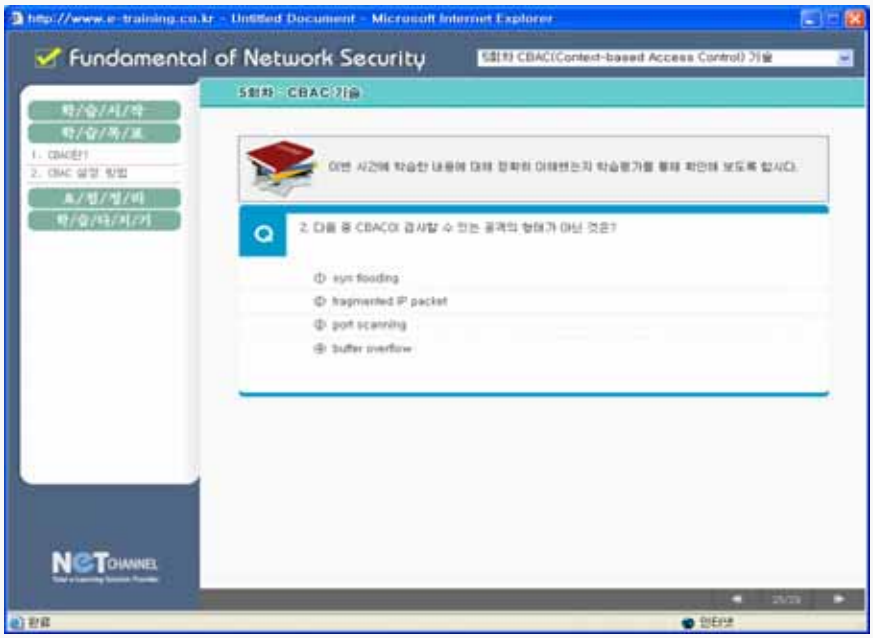

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 CBAC 2/3
CBAC 설정
라우터 인터페이스에의 검사 규칙과 ACL 적용 (Task 5)
세 개의 인터페이스를 가지고 있는 라우터에의 검사 규칙과 ACL 적용 예제
DMZ-bound Traffic
Inside
e0/0
Outside
e0/1
DMZ
e1/0
Router(config)# access-list 103 permit icmp host 172.16.0.2 any
Router(config)# access-list 103 deny ip any any
DMZ에서 발생한 ICMP 트래픽만을 허용한다.
Router(config)# access-list 104 permit icmp any host 172.16.0.2
Router(config)# access-list 104 permit tcp any host 172.16.0.2 eq www
Router(config)# access-list 104 deny ip any any
호스트 172.16.0.2로 향하는 라우터 출력 방향의 ICMP와 HTTP 트래픽만을 허용한다.
Router(config)# interface e1/0
Router(config-if)# ip access-group 103 in
Router(config-if)# ip access-group 104 out
외부 인터페이스의 라우터 입력 방향에 ACL과 검사 규칙을 적용한다.
20/29
완료
인터넷

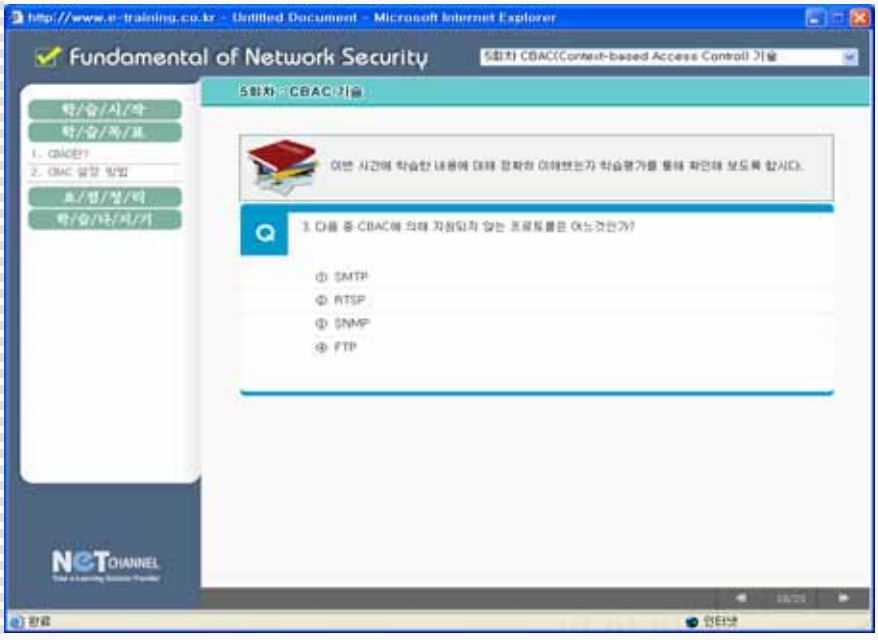

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 CBAC 실습
CBAC 설정
CBAC 테스트 및 확인 (Task 6)
show 명령어
Router#show ip inspect name inspection-name
Router#show ip inspect config
Router#show ip inspect interfaces
Router#show ip inspect session [detail]
Router#show ip inspect all
CBAC 설정, 인터페이스, 인터페이스 설정, 세션을 표시한다.
debug 명령어
Router(config)#debug ip inspect function-trace
Router(config)#debug ip inspect object-creation
Router(config)#debug ip inspect object-deletion
Router(config)#debug ip inspect events
Router(config)#debug ip inspect timers
일반적인 debug 명령어들의 입력 형식이다.
Router(config)#debug ip inspect protocol
특정 프로토콜에 관련된 debug 명령어 입력 형식이다.
해 설
감사 기능 추적, 감사 객체 생성/삭제, 감사 이벤트, 감사 타이머 등의 각종 CBAC 이벤트에 대한 메시지를 화면에 표시하기 위해서는 debug ip inspect 실행 명령어를 사용한다.
해 설
21/29
완료
인터넷

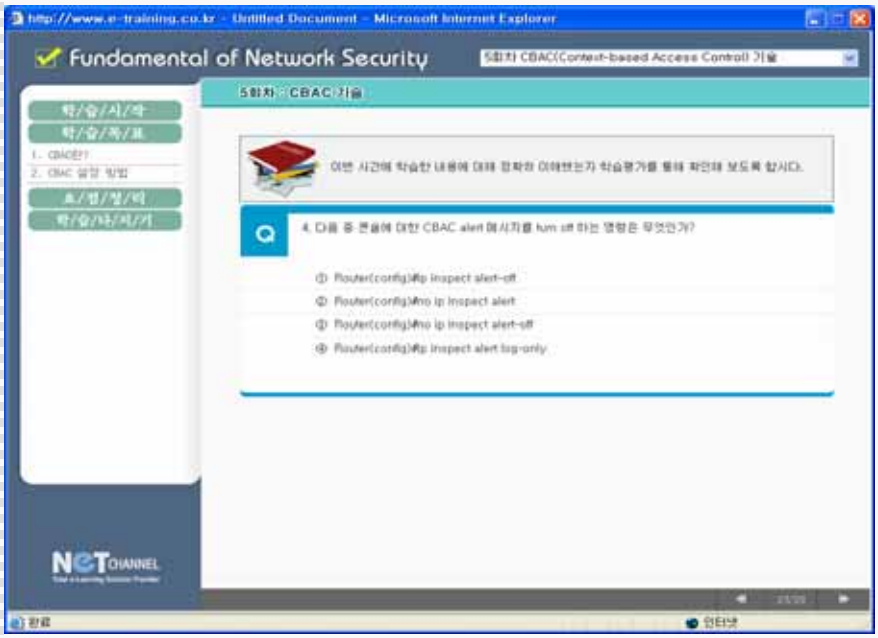

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 CBAC 실습
CBAC 설정
CBAC 테스트 및 확인 (Task 6)
CBAC 설정 제거 방법
Router(config)#no ip inspect
전체 CBAC 설정을 제거한다.
모든 전역 (global) timeouts과 thresholds 값을 디폴트 값으로 reset 한다.
설정되어 있는 모든 세션을 삭제한다.
연관된 (associated) 모든 dynamic ACL을 제거한다.
22/29
완료
인터넷

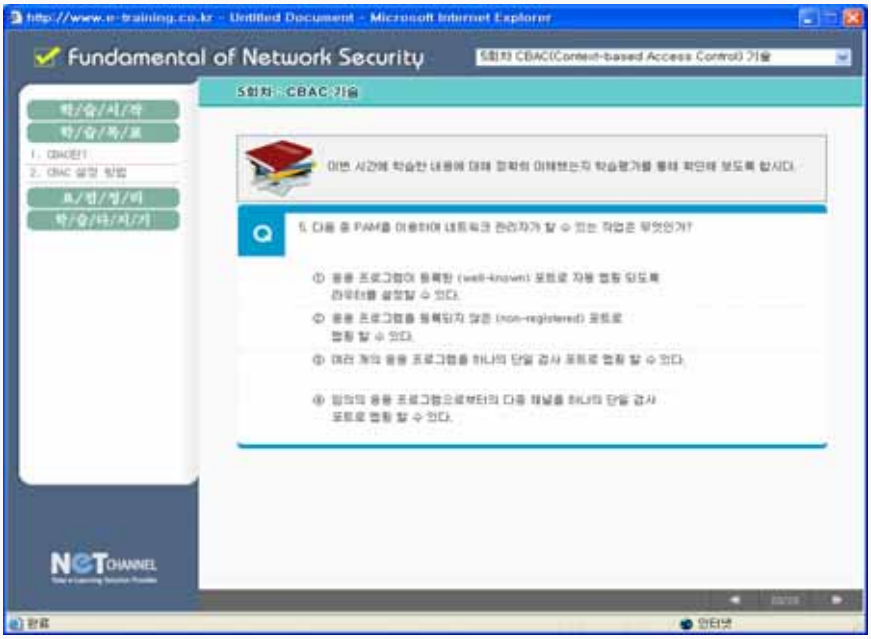

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
5회차 - CBAC 기술
Bootp는 UDP 프로토콜로서, Cisco 라우터에 의해 사용될 경우 Bootp 서비스를 제공하는 또다른 Cisco 라우터 상의 IOS 사본에 접속할 수 있게 되므로, 라우터 상의 Bootp server 기능은 제거하는 것이 바람직하다.
CBAC
CBAC의 동작
CBAC 설정 단계
• 감사 (audit trails) 기능과 경보 (alerts) 기능 설정
• Global timeouts과 thresholds 설정
• PAM
• 감사 규칙 정의
• 라우터 인터페이스에의 감사 규칙과 ACL 적용
• CBAC 테스트 및 확인
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
5회차 CBAC(Context-based Access Control) 기술
5회차 - CBAC 기술
1. CBAC란?
2. CBAC 설정 방법
① Extended audit
② CBAC
③ RSVP
④ Reactive filtering
NETCHANNEL
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
5회차 CBAC(Context-based Access Control) 기술
5회차 : CBAC 기술
2. 다음 중 CBAC이 검사할 수 있는 공격의 형태가 아닌 것은?
① syn flooding
② fragmented IP packet
③ port scanning
④ buffer overflow
NETCHANNEL


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
5회차 CBAC(Context-based Access Control) 기술
5회차 : CBAC 기술
3. 다음 중 CBAC에 의해 지원되지 않는 프로토콜은 어느것인가?
① SMTP
② RTSP
③ SNMP
④ FTP
NETCHANNEL


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
5회차 CBAC(Context-based Access Control) 기술
5회차 - CBAC 기술
NETCHANNEL


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
5회차 CBAC(Context-based Access Control) 기술
5회차 - CBAC 기술
NETCHANNEL

End of Lecture