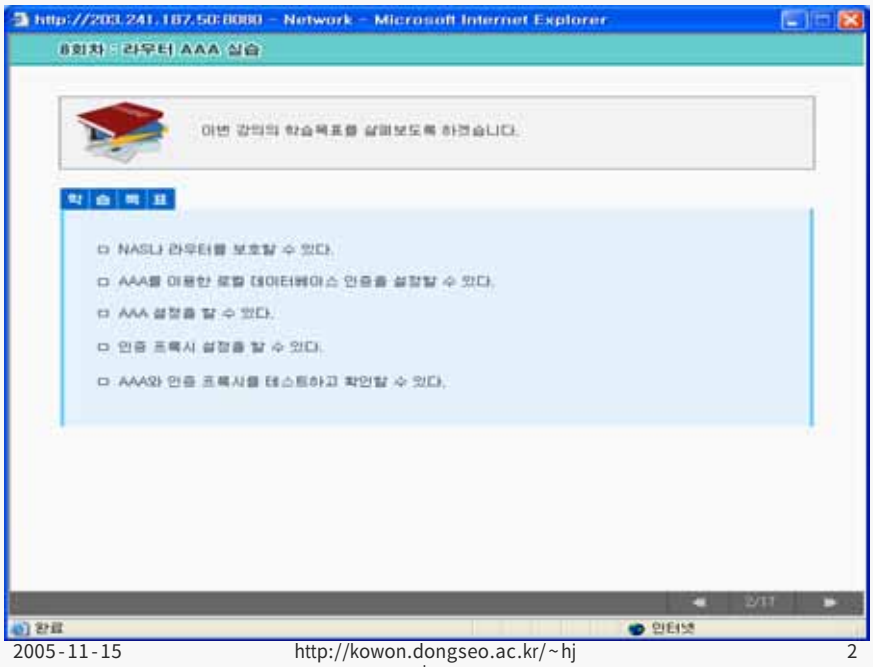
FNS

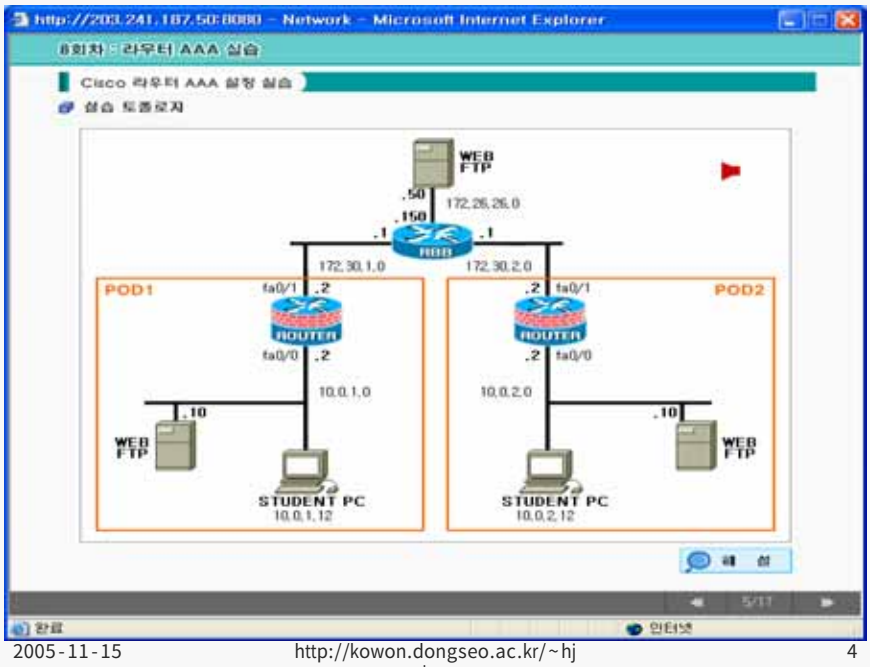
(Fundamental Network Security)

Ch8. 라우터 AAA 실습

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



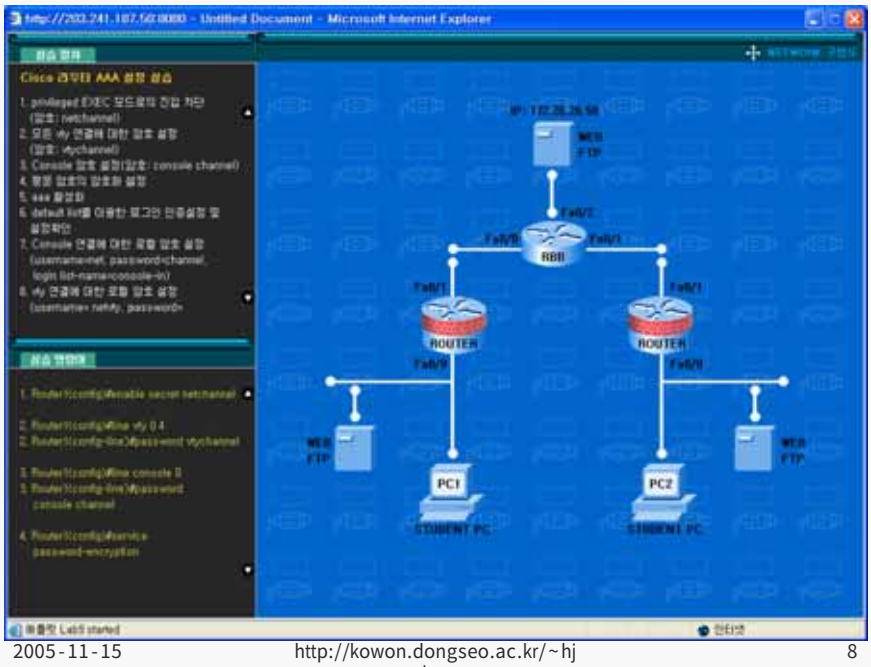

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
8회차 : 라우터 AAA 실습
Cisco 라우터 AAA 설정 실습
목 표
암호 설정을 통한 NAS 또는 라우터 보호 방법
AAA 인증 기능 수행을 위한 NAS 설정 방법
Privileged EXEC, vty, 콘솔 모드 접근 보안 및 테스트
AAA를 이용한 로컬 데이터베이스 인증 설정 방법
완료
인터넷

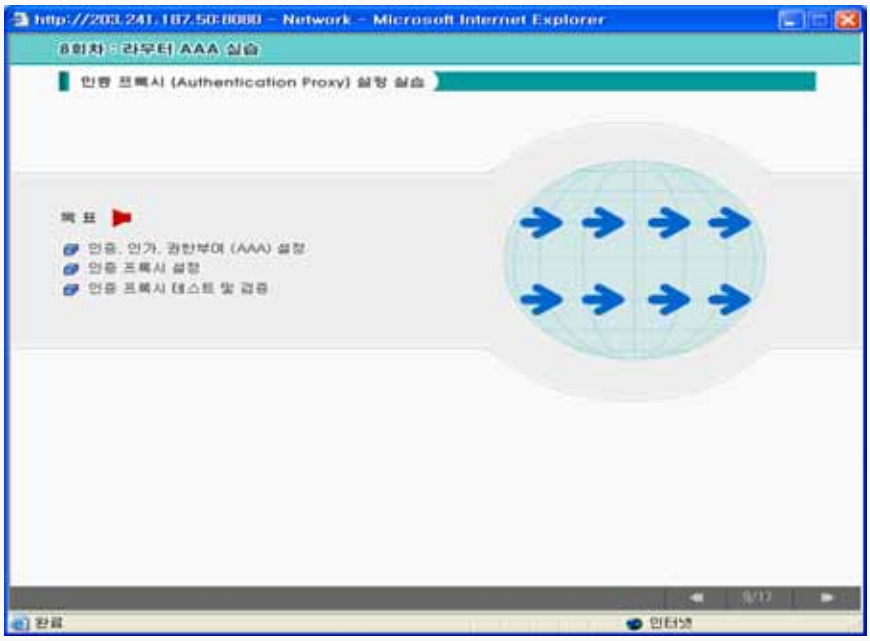

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
8회차 : 라우터 AAA 실습
Cisco 라우터 AAA 설정 실습
실습 토폴로지
WEB FTP
.50
.150
172.26.26.0
.1
.1
RBB
172.30.1.0
172.30.2.0
POD1
POD2
fa0/1
.2
ROUTER
fa0/0
.2
10.0.1.0
10.0.2.0
.10
WEB FTP
STUDENT PC
10.0.1.12
10.0.2.12
완료
인터넷

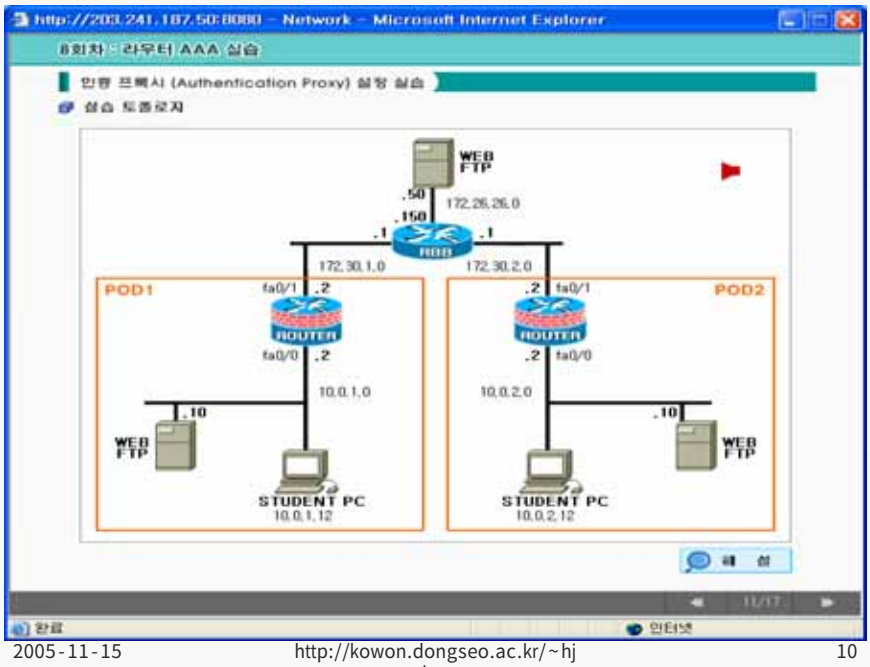

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
8회차 : 라우터 AAA 실습
Cisco 라우터 AAA 설정 실습
실습
제 1 단계: Privileged EXEC, vty, 콘솔 모드 접근성 보안 및 테스팅
암호 설정을 통하여 라우터 access point를 차단한다. 이를 위해 우선 netchannel이라는 password를 사용하여 privileged EXEC 모드에의 진입을 차단해 보자.(↵입력 후 Enter)
Router1(config)#enable secret netchannel
모든 vty 연결에 대한 password (vtychannel)를 설정한다.(↵입력 후 Enter)
Router1(config)#line vty 0 4
Router1(config-line)#password vtychannel
Console password (console channel)를 설정한다.(↵입력 후 Enter)
Router1(config)#line console 0
Router1(config-line)#password console channel
위에서 설정한 내용을 running configuration을 통하여 확인해보자. 모든 암호가 평문으로 보인다면 이를 암호화하기 위해서는 어떤 명령어를 사용해야 할까?(↵입력 후 Enter)
Router1(config)#service password-encryption
5/17
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
8회차 : 라우터 AAA 실습
Cisco 라우터 AAA 설정 실습
실습
제 2 단계: AAA를 이용한 로컬 데이터베이스 인증 설정 check
AAA 기능을 활성화 하기 위한 명령어를 입력한다.(↵입력 후 Enter)
Router1(config)#aaa new-model
Default list를 이용하여 enable password를 사용하기 위한 로그인 인증 설정 명령어를 입력한다.(↵입력 후 Enter)
Router1(config)#aaa authentication login default enable
이 명령어는 모든 로그인 액세스를 즉시 차단하게 되어 있다.
이제 위에서 설정한 모델을 테스트해보자. privileged mode 및 user mode에서 나와 다시 콘솔 포트로 라우터에 접근하고자 할 때 프롬프트가 제시한다.
여기서 입력해야 할 암호는 무엇일까?(↵입력 후 Enter)
정답: netchannel, enable secret password가 netchannel로 설정되어 있고 aaa 설정에서 default list를 enable password로 사용하도록 설정하였기 때문이다.
콘솔 연결에 대한 로컬 암호를 설정하는 명령어를 입력한다. 단, 여기서 username=net, password=channel를 사용하고, login list-name은 console-in을 사용한다.(↵입력 후 Enter)
Router1(config)#username net password channel
Router1(config)#aaa authentication login console-in local
Router1(config)#line console 0
Router1(config-line)#login authentication console-in
3/17
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
8회차 : 라우터 AAA 실습
Cisco 라우터 AAA 설정 실습
실습
제 2 단계: AAA를 이용한 로컬 데이터베이스 인증 설정
vty 연결에 대한 로컬 암호를 설정하는 명령어를 입력해보자.
단, 여기서 username=netvty, password=netvtychannel을 사용하고, login list-name은
vty-in을 사용한다.(※입력 후 Enter)
Router1(config)#username net password channel
Router1(config)#aaa authentication login console-in local
Router1(config)#line console 0
Router1(config-line)#login authentication console-in
제 3 단계: Debug를 이용한 연결 테스트
privileged 모드에서 debug 출력에 대한 올바른 timestamp 정보를 확인하기 위한 명령어와,
debug 메시지의 console logging 및 AAA 인증을 위한 debugging을 활성화 하는 명령어를
입력한다.(※입력 후 Enter)
Router1(config)#service timestamp debug datetime msec
Router1(config)#logging on
Router1(config)#logging console debugging
Router1#debug aaa authentication
aaa authentication 이벤트 트리거를 위해 콘솔 연결에서 일단 빠져 나온 후 다시 로그인 해본다.
또한 student PC로부터 Telnet 접속을 시도하여 debug aaa authentication 결과를 확인해본다.
실습하기
완료
인터넷


http://203.241.187.50:8080 - Untitled Document - Microsoft Internet Explorer
Cisco 라우터 AAA 설정 실습
WEB FTP
RBB
ROUTER
ROUTER
PC1
PC2
STUDENT PC
STUDENT PC
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
8회차 : 라우터 AAA 실습
인증 프록시 (Authentication Proxy) 설정 실습
목 표
인증, 인가, 권한부여 (AAA) 설정
인증 프록시 설정
인증 프록시 테스트 및 검증
5/17
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
8회차 : 라우터 AAA 실습
인증 프록시 (Authentication Proxy) 설정 실습
실습 토폴로지
WEB FTP
.50
.150
172.26.26.0
.1
.1
R0B
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
11/17
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
8회차 : 라우터 AAA 실습
인증 프록시 (Authentication Proxy) 설정 실습
실습
제 1 단계: Access Control Server 설정
본 실습을 위해서는 Access Control Server (ACS)를 사전에 설정해 놓을 필요가 있으며,
구체적으로 다음과 같이 설정한다.
• 인터페이스 설정에서 TACACS+와 auth-proxy를 설정한다.
• 설정은 group setup을 이용한다.
• auth-proxy의 custom attributes로 아래의 설정을 해 놓는다.
proxyacl#1=permit tcp any any
priv-lvl=15
제 2 단계: AAA 설정
AAA 기능을 활성화하고, 인증 및 인가 프로토콜을 명시하는 명령어를 입력한다.
(※입력 후 Enter)
Router1(config)#aaa new-model
Router1(config)#aaa authentication login default group tacacs+
Router1(config)#aaa authorization auth-proxy default group tacacs+
TACACS+ 서버와 서버에 사용할 key를 정의한다. 단,
TACACS+ 서버의 위치는 10.0.1.12이고, key 값으로는 netkey를 사용한다.(※입력 후 Enter)
Router1(config)#tacacs-server host 10.0.1.12
Router1(config)#tacacs-server key netkey
12/17
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
8회차 : 라우터 AAA 실습
인증 프록시 (Authentication Proxy) 설정 실습
실습
제 3 단계: ACL 설정
AAA 서버로부터 inside interface로 들어오는 TACACS+ 트래픽을 허용하고, 또한 외부로
나가는 (outbound) ICMP 트래픽과 FTP 및 WWW와 같은 CBAC 트래픽을 허용하며, 그 외의
모든 내부에서 발생한 트래픽은 차단하는 ACL을 정의한다 (ACL 번호: 101).(※입력 후 Enter)
Router1(config)#access-list 101 permit tcp host 10.0.1.12 eq tacacs host 10.0.1.2
Router1(config)#access-list 101 permit icmp any any
Router1(config)#access-list 101 permit tcp 10.0.1.0 0.0.0.255 any eq ftp
Router1(config)#access-list 101 permit tcp 10.0.1.0 0.0.0.255 any eq www
Router1(config)#access-list 101 deny ip any any
FTP 및 WWW와 같은 CBAC 트래픽의 내부 (inside) Web 또는 FTP 서버에 접근할 수 있도록
허용하고, 그 외의 모든 외부에서 발생된 트래픽은 차단하는 ACL을 정의한다
(ACL 번호: 102). (※입력 후 Enter)
Router1(config)#access-list 102 permit icmp any any
Router1(config)#access-list 102 permit tcp any host 10.0.1.12 eq ftp
Router1(config)#access-list 102 permit tcp any host 10.0.1.12 eq www
Router1(config)#access-list 102 deny ip any any
AAA 기능에 대한 라우터 HTTP 서버 기능을 활성화한다.(※입력 후 Enter)
Router1(config)#ip http server
Router1(config)#ip http authentication aaa
13/17
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
8회차 : 라우터 AAA 실습
인증 프록시 (Authentication Proxy) 설정 실습
실습
제 4 단계: 인증 프록시 설정
인증 프록시 규칙을 정의한다. 단, 인증 프록시 이름은 APRULE로 하고,
http auth-cache-time은 5로 한다.(※입력 후 Enter)
Router1(config)#ip auth-proxy name APRULE http auth-cache-time 5
인증 프록시 규칙을 내부 인터페이스 (inside interface)에 적용한다.(※입력 후 Enter)
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip auth-proxy APRULE
Router1(config)#ip access-group 101 in
ACL 102를 외부 인터페이스 (outside interface)에 적용한다.(※입력 후 Enter)
Router1(config)#interface fastethernet 0/1
Router1(config-if)#ip access-group 102 in
14/17
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
8회차 : 라우터 AAA 실습
인증 프록시 (Authentication Proxy) 설정 실습
실습
제 5 단계: 인증 프록시 테스트 및 검증
우선 앞에서 설정한 ACL을 확인해보자.(※입력 후 Enter)
Router1#show access-list
인증 프록시 설정을 확인해보자.(※입력 후 Enter)
Router1#show ip auth-proxy configuration
현재의 인증 프록시 설정에 대한 캐시를 확인해보자.(※입력 후 Enter)
Router1#show ip auth-proxy cache
ping 테스트 및 http 접속 시도 후의 인증 프록시 기능 테스트 및 검증 명령어.
http://172.26.26.50 (웹브라우저 강제시)
Router1#show access-list
Router1#show ip auth-proxy configuration
Router1#show ip auth-proxy cache
게시 판한
실습하기
15/17
완료
인터넷


http://203.241.187.50:8080 - Untitled Document - Microsoft Internet Explorer
인증 프록시 설정 실습
1. AAA 기능 활성화
2. 인증 및 인가 프로토콜 명시
3. TACACS+ 서버와 key 정의 (TACACS+ 서버 위치: 10.0.1.12, key 값: netkey1)
4. AAA 서버에서 inside interface로의 TACACS+ 트래픽을 허용하고, 외부로 나가는 ICMP 트래픽과 FTP 및 WWW 등의 CBAC 트래픽을 허용하고, 그 외의 모든 내부 트래픽을 차단하는 ACL (101번) 정의
5. vigor 라우팅 트래픽, 내부로 들어오는 (inbound) ICMP 트래픽, 그리고 FTP 및 WWW 등의 CBAC 트래픽의 내부 Web/FTP 서버 접근 허용, 그 외 모든 외부 트래픽을 차단하는 ACL (102번) 정의
실습 명령어
1. Router(config)#aaa new-model
2. Router(config)#aaa authentication login default group tacacs+
2. Router(config)#aaa authorization auth-proxy default group tacacs+
3. Router(config)#tacacs-server host 10.0.1.12
3. Router(config)#tacacs-server key netkey
4. Router(config)#access-list 101 permit tcp host 10.0.1.12 eq tacacs host 10.0.1.2
4. Router(config)#access-list 101 permit icmp any any
해줄힌 Lab9 started
인터넷
ROUTER
ROUTER
PC1
PC2
STUDENT PC
STUDENT PC


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
8회차 - 라우터 AAA 실습
지금까지 공부한 내용을 요약하여 다시 한번 정리를 하도록 하겠습니다.
부족한 부분은 다시 한번 확인 하시기 바랍니다.
Cisco 라우터 AAA 설정 실습
라우터에 간단한 암호 설정으로 NAS를 보호함으로써 네트워크 서버에 접근할 수 있는 사용자를 제어할 수 있고, 접근이 허용된 사용자가 이용할 수 있는 서비스를 제어할 수 있다.
네트워크 관리자는 인증, 인가, 계정 관리의 AAA 네트워크 보안 서비스 프레임워크를 이용하여 access control을 설정할 수 있는데,
구체적으로 AAA를 이용한 로컬 데이터베이스 인증 기능 설정 방법이 있다.
인증 프록시 설정 실습
인증 프록시 기능을 이용하여 사용자는 HTTP를 통한 네트워크 로그인이나 인터넷 액세스를 할 수 있다.
사용자의 특정 액세스 프로파일은 보통 Access Control Server로부터 자동적으로 제생되어 적용되는데,
이러한 사용자 프로파일은 인증된 사용자로부터의 특정 트래픽이 발생할 경우에만 활성화된다.
이를 위한 설정 작업은 아래의 다섯 단계를 통하여 수행할 수 있다.
제 1 단계: Access Control Server 설정
제 2 단계: AAA 설정
제 3 단계: ACL 설정
제 4 단계: 인증 프록시 설정
제 5 단계: 인증 프록시 테스트 및 검증
16/17
완료
인터넷

End of Lecture