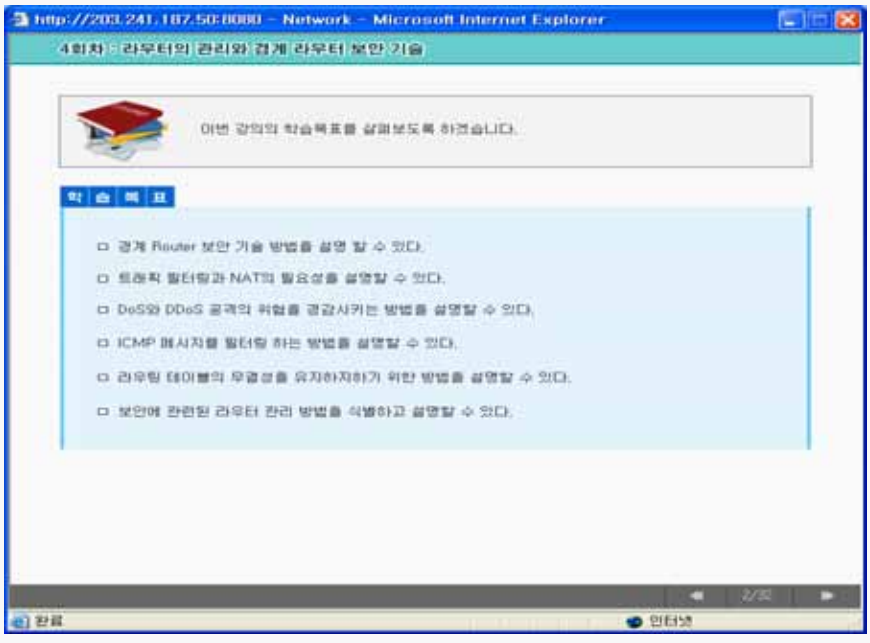
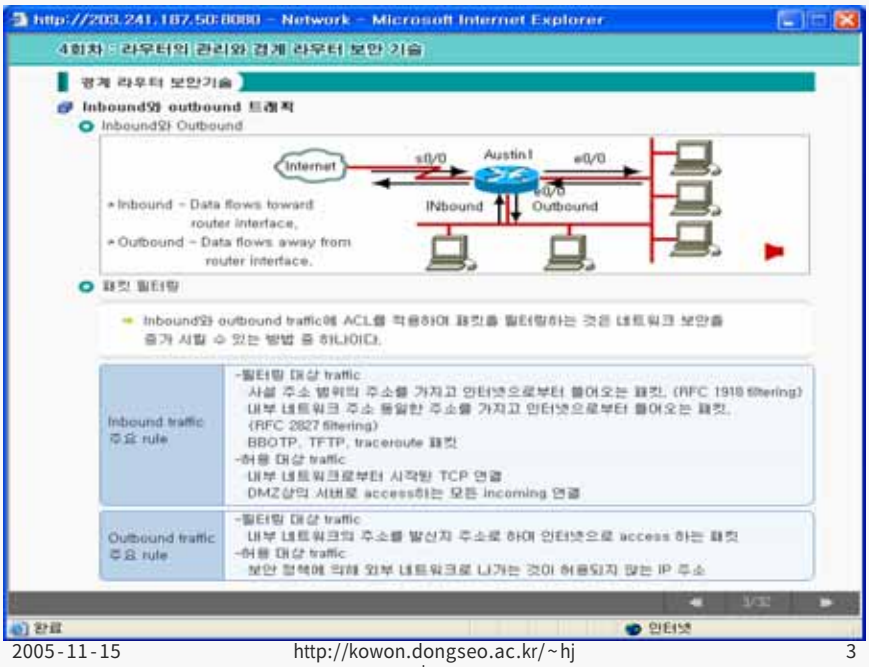
FNS

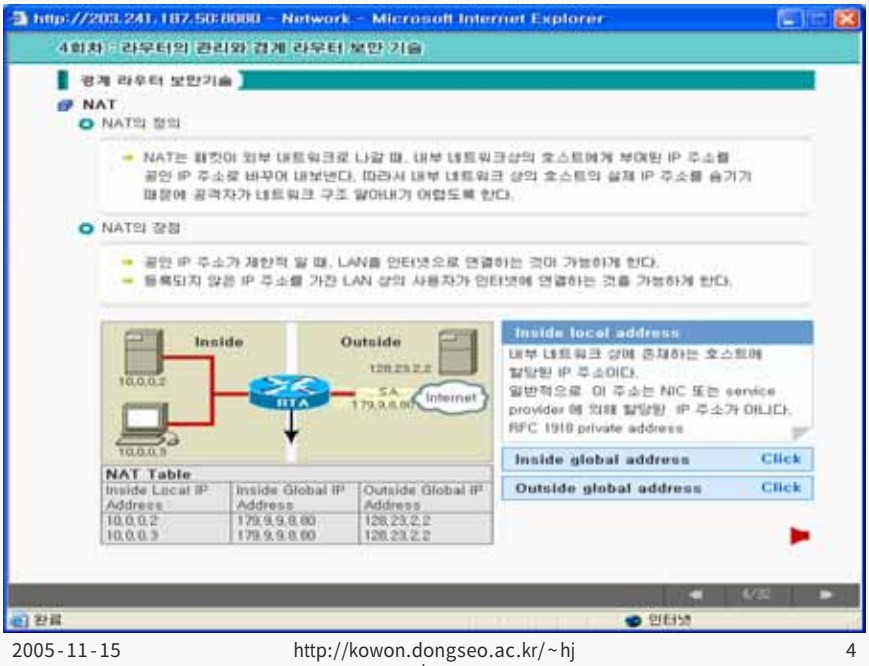
(Fundamental Network Security)

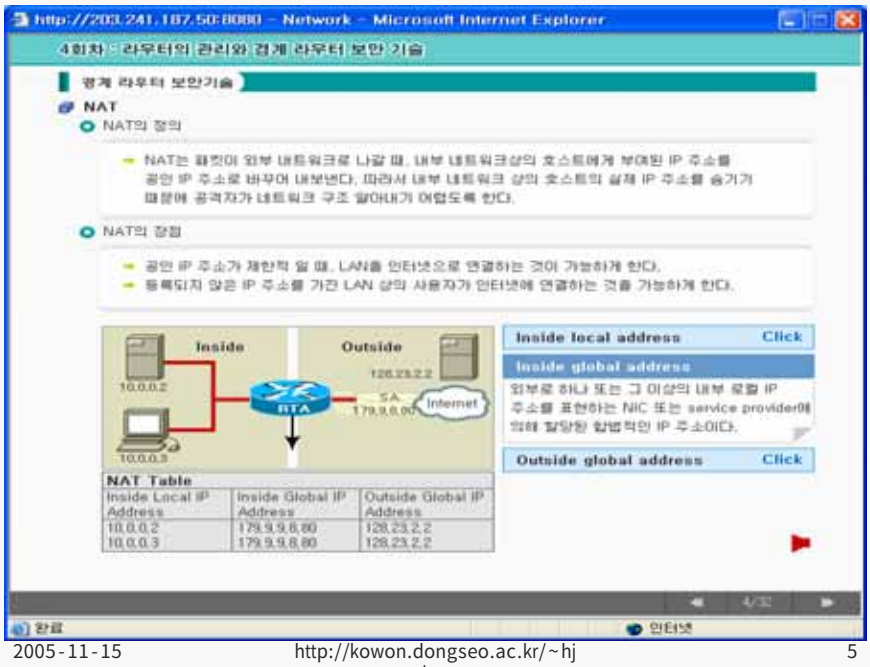
Ch4. 라우터의 관리와 경계라우터 보안 기술

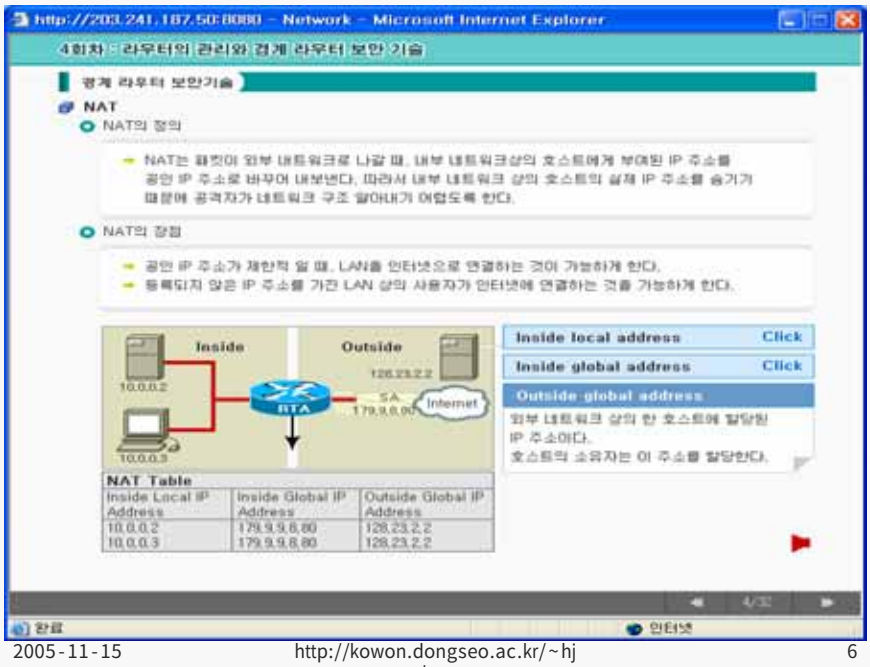
동서대학교/인터넷공학부
이 훈 재
hjlee@dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee
http://crypto.dongseo.ac.kr

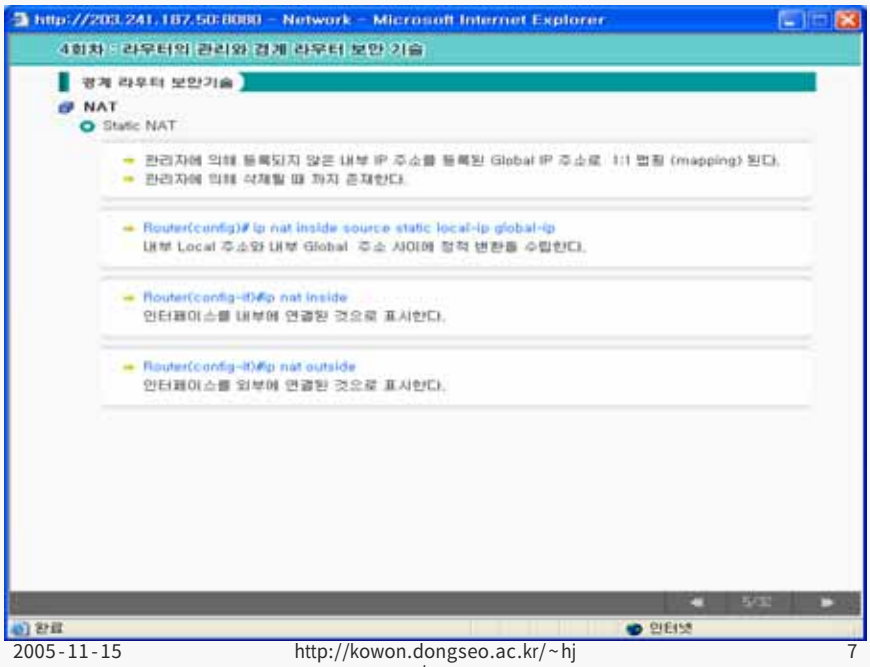


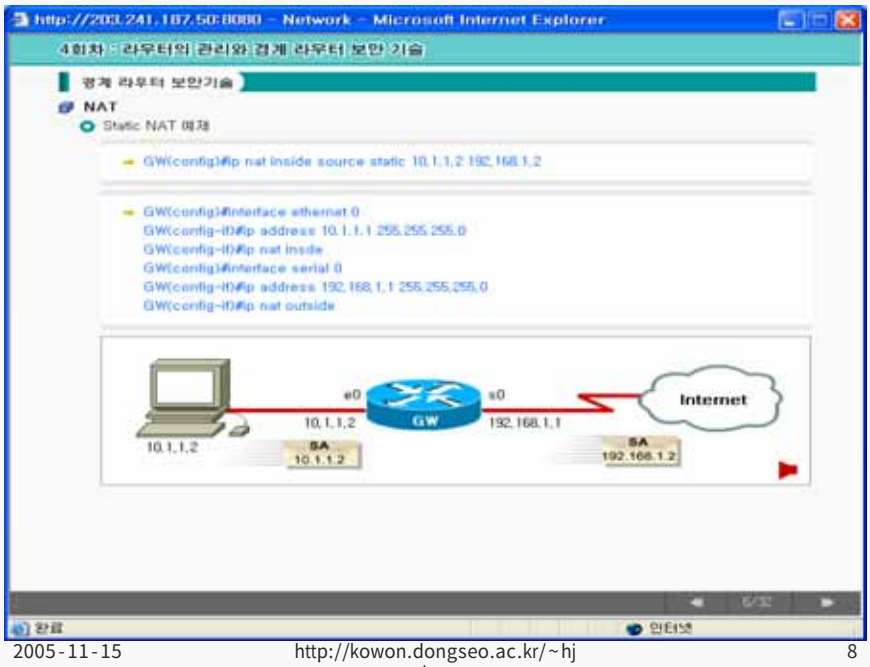

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
Inbound와 outbound 트래픽
Inbound와 Outbound
Internet
s0/0
Austin1
e0/0
s0/0
INbound
Outbound
• Inbound - Data flows toward router interface,
• Outbound - Data flows away from router interface.
패킷 필터링
Inbound와 outbound traffic에 ACL을 적용하여 패킷을 필터링하는 것은 네트워크 보안을 증가 시킬 수 있는 방법 중 하나이다.
Inbound traffic 주요 rule
-필터링 대상 traffic
사설 주소 범위의 주소를 가지고 인터넷으로부터 들어오는 패킷. (RFC 1918 filtering)
내부 네트워크 주소 동일한 주소를 가지고 인터넷으로부터 들어오는 패킷.
(RFC 2827 filtering)
BBOTP, TFTP, traceroute 패킷
-허용 대상 traffic
내부 네트워크로부터 시작된 TCP 연결
DMZ상의 서버로 access하는 모든 incoming 연결
Outbound traffic 주요 rule
-필터링 대상 traffic
내부 네트워크의 주소를 발신자 주소로 하여 인터넷으로 access 하는 패킷
-허용 대상 traffic
보안 정책에 의해 외부 네트워크로 나가는 것이 허용되지 않는 IP 주소
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
NAT
NAT의 정의
NAT는 패킷이 외부 네트워크로 나갈 때, 내부 네트워크상의 호스트에게 부여된 IP 주소를 공인 IP 주소로 바꾸어 내보낸다. 따라서 내부 네트워크 상의 호스트의 실제 IP 주소를 숨기기 때문에 공격자가 네트워크 구조 알아내기 어렵도록 한다.
NAT의 장점
공인 IP 주소가 제한적 일 때, LAN을 인터넷으로 연결하는 것이 가능하게 한다.
등록되지 않은 IP 주소를 가진 LAN 상의 사용자가 인터넷에 연결하는 것을 가능하게 한다.
Inside
Outside
10.0.0.2
10.0.0.3
128.23.2.2
NAT
SA
179.9.8.80
Internet
Inside local address
내부 네트워크 상에 존재하는 호스트에 할당된 IP 주소이다.
일반적으로 이 주소는 NIC 또는 service provider 에 의해 할당된 IP 주소가 아니다.
RFC 1918 private address
Inside global address Click
Outside global address Click
NAT Table
Inside Local IP Address
Inside Global IP Address
Outside Global IP Address
10.0.0.2 179.9.9.8.80 128.23.2.2
10.0.0.3 179.9.9.8.80 128.23.2.2
완료
인터넷

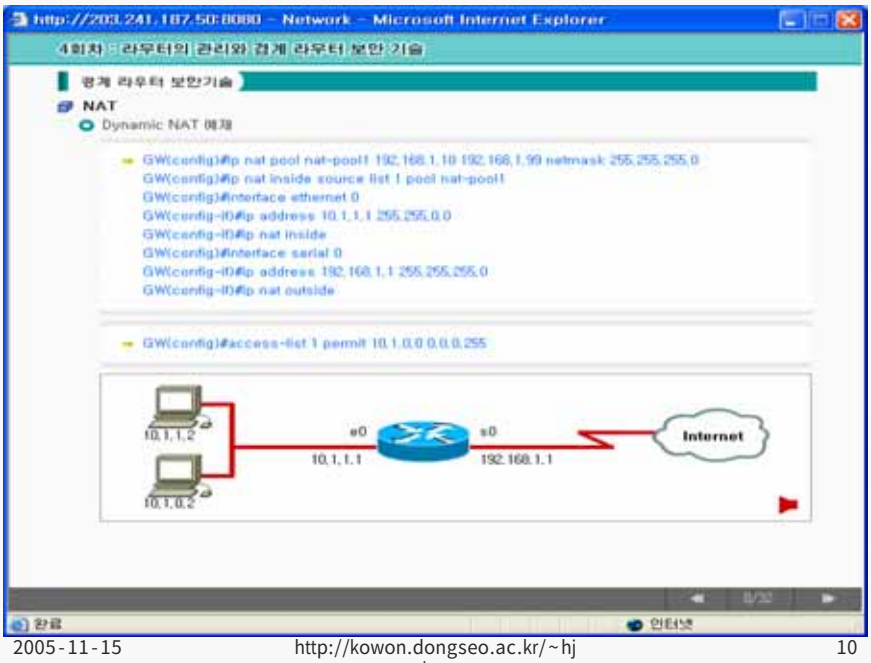

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
NAT
NAT의 정의
NAT는 패킷이 외부 네트워크로 나갈 때, 내부 네트워크상의 호스트에게 부여된 IP 주소를 공인 IP 주소로 바꾸어 내보낸다. 따라서 내부 네트워크 상의 호스트의 실제 IP 주소를 숨기기 때문에 공격자가 네트워크 구조 알아내기 어렵도록 한다.
NAT의 장점
공인 IP 주소가 제한적 일 때, LAN을 인터넷으로 연결하는 것이 가능하게 한다.
등록되지 않은 IP 주소를 가진 LAN 상의 사용자가 인터넷에 연결하는 것을 가능하게 한다.
Inside
Outside
Internet
Inside local address
Click
Inside global address
외부로 하나 또는 그 이상의 내부 로컬 IP 주소를 표현하는 NIC 또는 service provider에 의해 할당된 합법적인 IP 주소이다.
Outside global address
Click
NAT Table
Inside Local IP Address
Inside Global IP Address
Outside Global IP Address
10.0.0.2
179.9.9.8.80
128.23.2.2
10.0.0.3
179.9.9.8.80
128.23.2.2
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
NAT
NAT의 정의
NAT는 패킷이 외부 네트워크로 나갈 때, 내부 네트워크상의 호스트에게 부여된 IP 주소를 공인 IP 주소로 바꾸어 내보낸다. 따라서 내부 네트워크 상의 호스트의 실제 IP 주소를 숨기기 때문에 공격자가 네트워크 구조 알아내기 어렵도록 한다.
NAT의 장점
공인 IP 주소가 제한적 일 때, LAN을 인터넷으로 연결하는 것이 가능하게 한다.
등록되지 않은 IP 주소를 가진 LAN 상의 사용자가 인터넷에 연결하는 것을 가능하게 한다.
Inside
Outside
Internet
Inside local address
Click
Inside global address
Click
Outside global address
외부 네트워크 상의 한 호스트에 할당된 IP 주소이다.
호스트의 소유자는 이 주소를 할당한다.
NAT Table
Inside Local IP Address
Inside Global IP Address
Outside Global IP Address
10.0.0.2
179.9.9.8.80
128.23.2.2
10.0.0.3
179.9.9.8.80
128.23.2.2
완료
인터넷

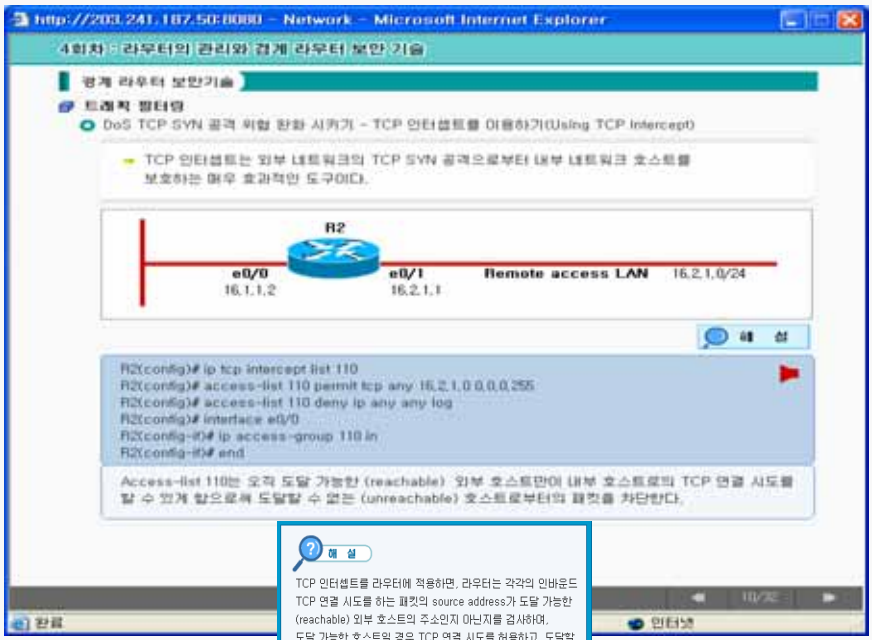

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
NAT
Static NAT
관리자에 의해 등록되지 않은 내부 IP 주소를 등록된 Global IP 주소로 1:1 맵핑 (mapping) 된다.
관리자에 의해 삭제될 때 까지 존재한다.
Router(config)# ip nat inside source static local-ip global-ip
내부 Local 주소와 내부 Global 주소 사이에 정적 변환을 수립한다.
Router(config-if)#ip nat inside
인터페이스를 내부에 연결된 것으로 표시한다.
Router(config-if)#ip nat outside
인터페이스를 외부에 연결된 것으로 표시한다.
완료
인터넷

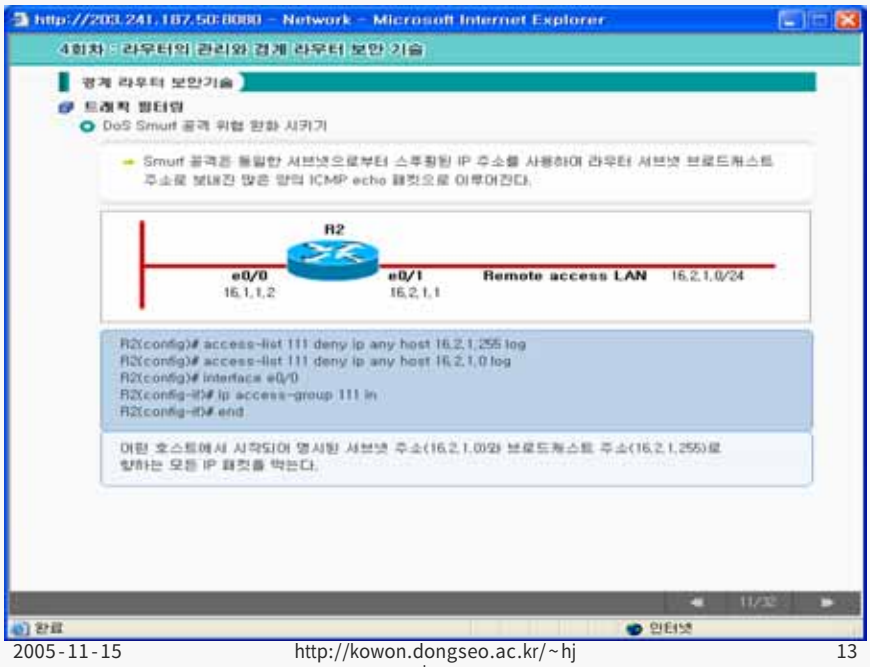

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
NAT
Static NAT 예제
GW(config)#ip nat inside source static 10.1.1.2 192.168.1.2
GW(config)#interface ethernet 0
GW(config-if)#ip address 10.1.1.1 255.255.255.0
GW(config-if)#ip nat inside
GW(config)#interface serial 0
GW(config-if)#ip address 192.168.1.1 255.255.255.0
GW(config-if)#ip nat outside
e0
10.1.1.2
GW
s0
192.168.1.1
Internet
10.1.1.2
SA
10.1.1.2
SA
192.168.1.2
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
NAT
Dynamic NAT
등록되지 않은 내부 IP 주소를 등록된 IP 주소 그룹으로부터 IP 주소를 선택하여 변환시킨다.
Router(config)# ip nat pool name start-ip end-ip {netmask
netmask | prefix-length prefix-length}
할당될 Global 주소 영역을 설정한다.
Router(config-if)#access-list
변환될 IP 주소를 ACL로 정의한다
완료
인터넷

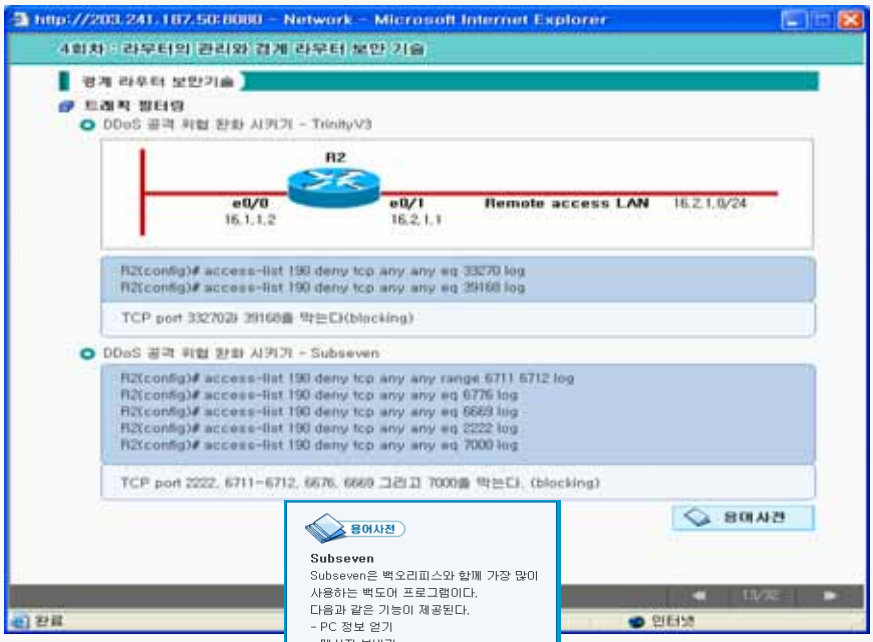

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
NAT
Dynamic NAT 예제
GW(config)#ip nat pool nat-pool1 192.168.1.10 192.168.1.99 netmask 255.255.255.0
GW(config)#ip nat inside source list 1 pool nat-pool1
GW(config)#interface ethernet 0
GW(config-if)#ip address 10.1.1.1 255.255.0.0
GW(config-if)#ip nat inside
GW(config)#interface sarial 0
GW(config-if)#ip address 192.168.1.1 255.255.255.0
GW(config-if)#ip nat outside
GW(config)#access-list 1 permit 10.1.0.0 0.0.0.255
10.1.1.2
10.1.0.2
e0
10.1.1.1
s0
192.168.1.1
Internet
완료
인터넷

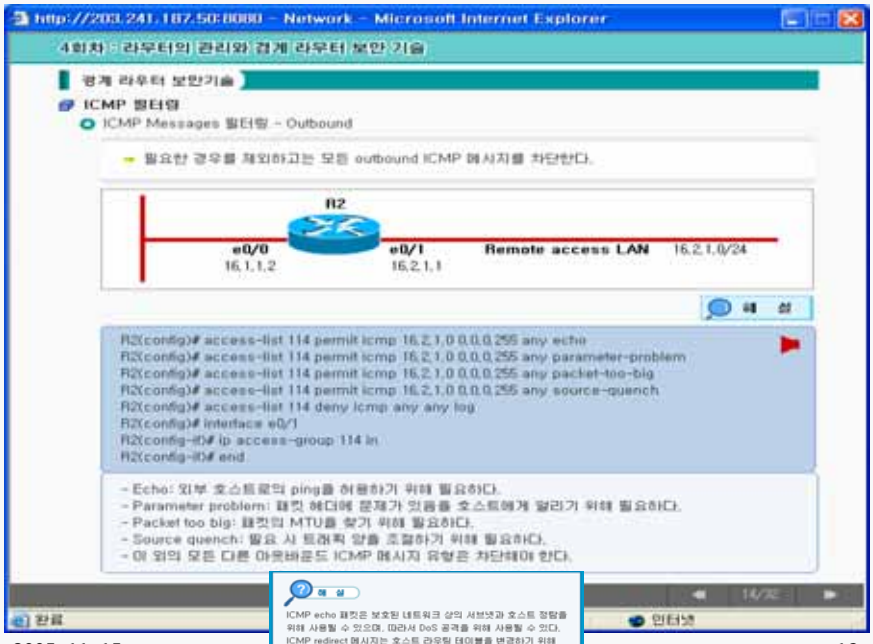

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
트래픽 필터링
DoS TCP SYN 공격 위협 완화 시키기 - 외부 access 막기(Blocking External Access)
TCP SYN 공격은 외부 네트워크로부터 SYN flag 만이 설정된 많은 양의 패킷들을 내부 네트워크로 전송하여 수신 노드의 연결 큐(connection queue)를 포화시킴으로써 네트워크 자원을 점유한다.
R2
e0/0
16.1.1.2
e0/1
16.2.1.1
Remote access LAN
16.2.1.0/24
해 설
R2(config)# access-list 109 permit tcp any 16.2.1.0 0.0.0.255 established
R2(config)# access-list 109 deny ip any any log
R2(config)# interface e0/0
R2(config-if)# ip access-group 109 in
R2(config-if)# end
TCP 세션이 설정된 트래픽 만을 허용하고 그 외의 모든 트래픽을 차단하도록 함으로써 SYN flag만이 설정된 inbound 패킷을 허용하지 않는다.
해 설
그림은 Corporate LAN의 일부이다. 즉, e0/0과 e0/1은 모두 내부 네트워크에 속하는 인터페이스로서 16.2.1.0/24의 네트워크를 remote access LAN으로 설정한 경우이다. 이 경우 외부 네트워크로부터 SYN flag만이 설정된 인바운드 트래픽이 라우터 R2를 통과하지 못하도록 하되, 내부 네트워크로부터 발생한 request에 대한 외부 네트워크로부터의 response는 (즉, TCP 세션이 established 된 경우는) 허용하도록 하는 것이 DoS TCP SYN 공격 위협을 방지하는 것이다.
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
트래픽 필터링
DoS TCP SYN 공격 위협 완화 시키기 - TCP 인터셉트를 이용하기(Using TCP Intercept)
TCP 인터셉트는 외부 네트워크의 TCP SYN 공격으로부터 내부 네트워크 호스트를 보호하는 매우 효과적인 도구이다.
R2
e0/0
16.1.1.2
e0/1
16.2.1.1
Remote access LAN
16.2.1.0/24
해 설
R2(config)# ip tcp intercept list 110
R2(config)# access-list 110 permit tcp any 16.2.1.0 0.0.0.255
R2(config)# access-list 110 deny ip any any log
R2(config)# interface e0/0
R2(config-if)# ip access-group 110 in
R2(config-if)# end
Access-list 110는 오직 도달 가능한 (reachable) 외부 호스트만이 내부 호스트로의 TCP 연결 시도를 할 수 있게 함으로써 도달할 수 없는 (unreachable) 호스트로부터의 패킷을 차단한다.
해 설
TCP 인터셉트를 라우터에 적용하면, 라우터는 각각의 인바운드 TCP 연결 시도를 하는 패킷의 source address가 도달 가능한 (reachable) 외부 호스트의 주소인지 아닌지를 검사하여, 도달 가능한 호스트일 경우 TCP 연결 시도를 허용하고, 도달할 수 없는 (unreachable) 호스트일 경우에는 TCP 연결 시도를 차단한다.
완료
인터넷

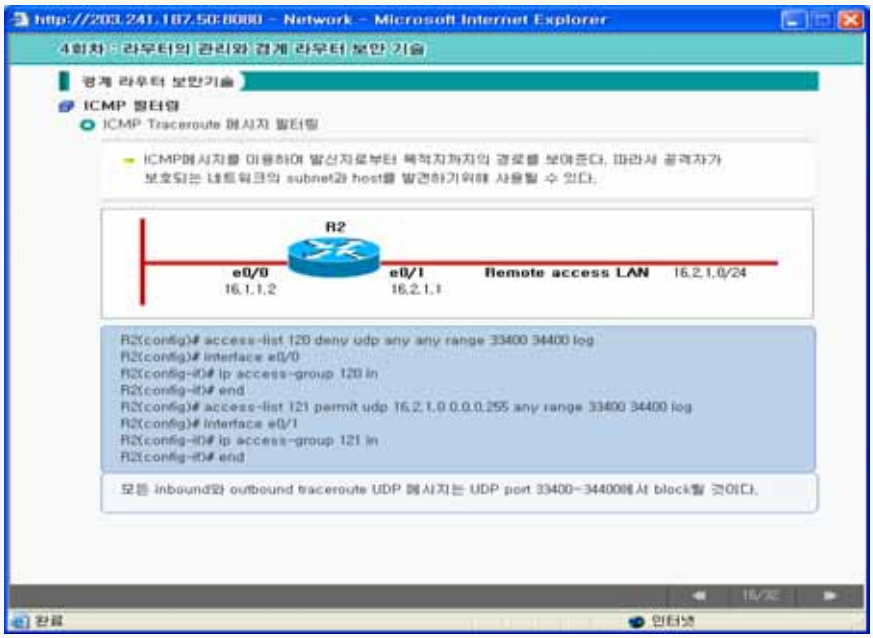

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 - 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
트래픽 필터링
DoS Smurf 공격 위협 완화 시키기
Smurf 공격은 동일한 서브넷으로부터 스푸핑된 IP 주소를 사용하여 라우터 서브넷 브로드캐스트 주소로 보내진 많은 양의 ICMP echo 패킷으로 이루어진다.
R2
e0/0
16.1.1.2
e0/1
16.2.1.1
Remote access LAN
16.2.1.0/24
R2(config)# access-list 111 deny ip any host 16.2.1.255 log
R2(config)# access-list 111 deny ip any host 16.2.1.0 log
R2(config)# interface e0/0
R2(config-if)# ip access-group 111 in
R2(config-if)# end
이런 호스트에서 시작되어 명시된 서브넷 주소(16.2.1.0)와 브로드캐스트 주소(16.2.1.255)로 향하는 모든 IP 패킷을 막는다.
11/32
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 - 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
트래픽 필터링
DDoS 공격 위협 완화 시키기 - TRIN00
DDoS 공격을 예방할 수 없으나 알려진 공격 port를 filter 하는 ACL을 구성하는 것에 의해 많은 발생을 경감시킬 수 있다.
R2
e0/0
16.1.1.2
e0/1
16.2.1.1
Remote access LAN
16.2.1.0/24
R2(config)# access-list 100 deny tcp any any eq 27665 log
R2(config)# access-list 100 deny udp any any eq 31335 log
R2(config)# access-list 100 deny udp any any eq 27444 log
TCP port 27665와 UDP port 31335와 27444를 막는다(blocking)
DDoS 공격 위협 완화 시키기 - Stacheldraht
R2(config)# access-list 100 deny tcp any any eq 16660 log
R2(config)# access-list 100 deny tcp any any eq 65000 log
TCP port 16660과 65000을 막는다(blocking)
용어사전
TRIN00
인터넷 해킹에 대해 크게 이슈화 되었던 대표적 분산 서비스 공격이다.
중앙의 통제 center에서 인터넷에 공개된 여러 서버들의 보안 홀을 침투하여 공격을 위한 agent들을 구축한 뒤, 특정 방식의 명령 통제하에 있는 agent들은 공격 명령을 수행하게 된다. master에 의해 통제하에 놓인 해당 agent들은 무차별 UDP Flooding을 공격대상 호스트로 보냄으로써 대상 호스트를 서비스 불능 상태로 만든다.
Stacheldraht
trinoo의 네트워크 구조와 TFN의 다양한 공격방법 그리고 Communication 상의 encryption 기능을 포함한 DDoS 공격이다. 암호화를 위해서 공격자가 직접 사용하는 telnet과 비슷한 프로그램을 제공하는데 이프로그램이 Attacker와 Master 간의 암호화된 통신을 보장한다. 따라서 Attacker와 Master간의 통신에 대해서는 네트워크 패킷을 분석한다 해도 Stacheldraht 의 여부를 판단하기가 쉽지 않다.
해 설
일반적으로 라우터는 DDoS 공격을 예방할 수는 없으나, 알려진 공격 포트를 필터링하는 access-list를 설정해 놓음으로써 DDoS 공격의 발생 횟수를 감소시킬 수는 있다.
이러한 DDoS 공격 에이전트 (또는 공격 도구) 중 현재 잘 알려져 있는 것으로는 TRIN00, Stacheldraht, TrinityV3, Subseven 등이 있으며, 이들은 특정 TCP 또는 UDP 포트를 막음으로써 공격 위협을 격감할 수 있다.


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
트래픽 필터링
DDoS 공격 위협 완화 시키기 - TrinityV3
R2
e0/0
16.1.1.2
e0/1
16.2.1.1
Remote access LAN
16.2.1.0/24
R2(config)# access-list 190 deny tcp any any eq 33270 log
R2(config)# access-list 190 deny tcp any any eq 39168 log
TCP port 33270과 39168을 막는다(blocking)
DDoS 공격 위협 완화 시키기 - Subseven
R2(config)# access-list 190 deny tcp any any range 6711 6712 log
R2(config)# access-list 190 deny tcp any any eq 6776 log
R2(config)# access-list 190 deny tcp any any eq 6669 log
R2(config)# access-list 190 deny tcp any any eq 2222 log
R2(config)# access-list 190 deny tcp any any eq 7000 log
TCP port 2222, 6711~6712, 6776, 6669 그리고 7000을 막는다. (blocking)
용어사전
용어사전
Subseven
Subseven은 백오리피스와 함께 가장 많이 사용하는 백도어 프로그램이다.
다음과 같은 기능이 제공된다.
- PC 정보 얻기
- 메시지 보내기
- 파일 찾기
- 파일 복사, 이동, 삭제
13/32
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
ICMP 필터링
ICMP Messages 필터링 - Outbound
필요한 경우를 제외하고는 모든 outbound ICMP 메시지를 차단한다.
R2
e0/0
16.1.1.2
e0/1
16.2.1.1
Remote access LAN
16.2.1.0/24
해 설
R2(config)# access-list 114 permit icmp 16.2.1.0 0.0.0.255 any echo
R2(config)# access-list 114 permit icmp 16.2.1.0 0.0.0.255 any parameter-problem
R2(config)# access-list 114 permit icmp 16.2.1.0 0.0.0.255 any packet-too-big
R2(config)# access-list 114 permit icmp 16.2.1.0 0.0.0.255 any source-quench
R2(config)# access-list 114 deny icmp any any log
R2(config)# interface e0/1
R2(config-if)# ip access-group 114 in
R2(config-if)# end
- Echo: 외부 호스트로의 ping을 허용하기 위해 필요하다.
- Parameter problem: 패킷 헤더에 문제가 있음을 호스트에게 알리기 위해 필요하다.
- Packet too big: 패킷의 MTU를 찾기 위해 필요하다.
- Source quench: 필요 시 트래픽 양을 조절하기 위해 필요하다.
- 이 외의 모든 다른 아웃바운드 ICMP 메시지 유형은 차단해야 한다.
해 설
ICMP echo 패킷은 보호된 네트워크 상의 서브넷과 호스트 정탐을 위해 사용될 수 있으며, 따라서 DoS 공격을 위해 사용될 수 있다. ICMP redirect 메시지는 호스트 라우팅 테이블을 변경하기 위해 사용될 수 있다. 따라서 이들은 꼭 필요한 경우를 제외하고는 라우터의 e0/1 인터페이스의 인바운드 방향에서 차단하여 외부로 나가지 못하게 해야한다.
14/32
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
ICMP 필터링
ICMP Messages 필터링 – Inbound
필요한 경우를 제외하고는 모든 inbound ICMP 메시지를 차단한다.
R2
e0/0
16.1.1.2
e0/1
16.2.1.1
Remote access LAN
16.2.1.0/24
해 설
R2(config)# access-list 112 deny icmp any any echo log
R2(config)# access-list 112 deny icmp any any redirect log
R2(config)# access-list 112 deny icmp any any mask-request log
R2(config)# access-list 112 permit icmp any 16.2.1.0 0.0.0.255
R2(config)# interface e0/0
R2(config-if)# ip access-group 112 in
R2(config-if)# end
- 모든 ICMP echo와 redirect 메시지를 막는다.
- 추가적으로 mask-request 메시지도 막는다.
- 그 외의 16.2.1.0/24 네트워크로의 인바운드 ICMP 메시지는 허용한다.
해 설
ICMP echo 패킷은 보호된 네트워크 상의 서브넷과 호스트 정탐을 위해 사용될 수 있으며, 따라서 DoS 공격을 위해 사용될 수 있다. ICMP redirect 메시지는 호스트 라우팅 테이블을 변경하기 위해 사용될 수 있다. 따라서 이들은 라우터의 e0/0 인터페이스의 인바운드 방향에서 차단하여 remote access LAN으로 들어오지 못하게 해야 한다.
완료
인터넷

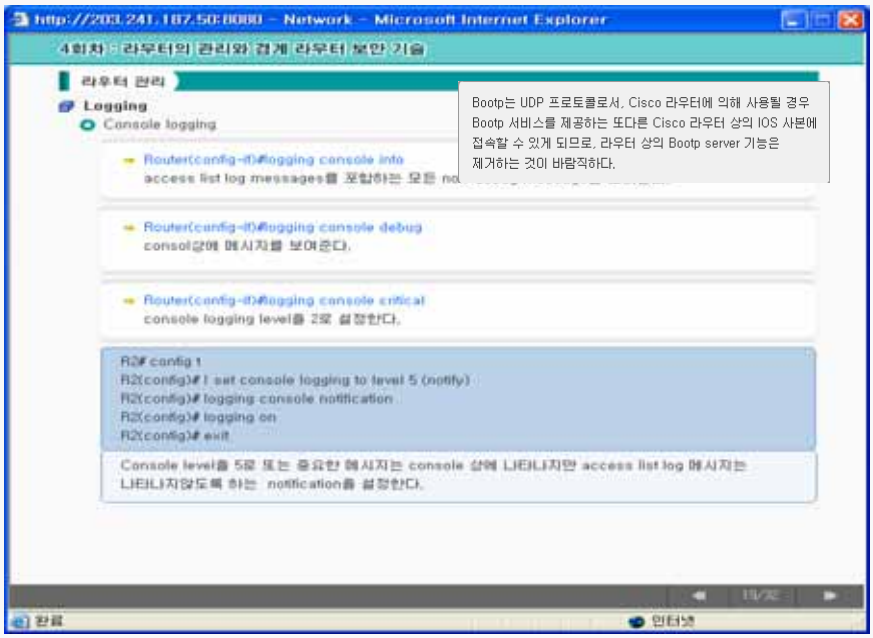

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
ICMP 필터링
ICMP Traceroute 메시지 필터링
ICMP메시지를 이용하여 발신지로부터 목적지까지의 경로를 보여준다. 따라서 공격자가 보호되는 네트워크의 subnet과 host를 발견하기위해 사용될 수 있다.
R2
e0/0
16.1.1.2
e0/1
16.2.1.1
Remote access LAN
16.2.1.0/24
R2(config)# access-list 120 deny udp any any range 33400 34400 log
R2(config)# interface e0/0
R2(config-if)# ip access-group 120 in
R2(config-if)# end
R2(config)# access-list 121 permit udp 16.2.1.0 0.0.0.255 any range 33400 34400 log
R2(config)# interface e0/1
R2(config-if)# ip access-group 121 in
R2(config-if)# end
모든 inbound와 outbound traceroute UDP 메시지는 UDP port 33400~34400에서 block될 것이다.
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
라우팅 테이블 보호 하기
라우팅 테이블 무결성
공격자는 보호되지 않은 라우터로 거짓 라우팅 update 패킷을 보내 라우팅 테이블에 오류를 발생하게 할 수 있다.
라우팅 테이블 무결성을 보호하기위한 방법
Static Route 만을 사용한다.
• 소규모 네트워크에서는 가능하지만 대규모 네트워크에서는 부적당하다.
• 주어진 목적지로 단 하나의 경로 라우터에 수동으로 설정된다.
• Route update 패킷을 교환하지 않기 때문에 spoofing 공격에 취약하지 않다.
Route table update를 인증한다. Click
Passive interface를 사용한다. Click
router(config)#key-string
상대방 라우터와 교환되는 message digest 또는 hash를 생성하는데 사용되는 MD5 key를 정의한다.
완료
인터넷

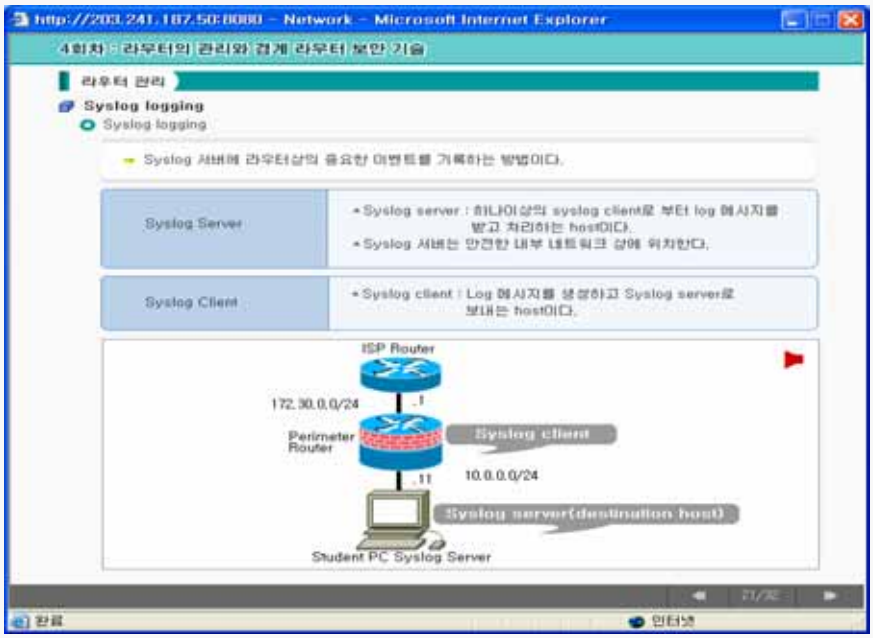

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
라우팅 테이블 보호 하기
라우팅 테이블 무결성
공격자는 보호되지 않은 라우터로 거짓 라우팅 update 패킷을 보내 라우팅 테이블에 오류를 발생하게 할 수 있다.
라우팅 테이블 무결성을 보호하기위한 방법
Static Route 만을 사용한다. Click
Route table update를 인증한다.
• Cisco IOS 소프트웨어는 다음의 라우팅 프로토콜에 대해 라우팅 프로토콜 update의 MD5 인증을 사용한다.
• RIPv2
• OSPF
• Enhanced IGRP
• BGP
Passive interface를 사용한다. Click
router(config)#key-string
상대방 라우터와 교환되는 message digest 또는 hash를 생성하는데 사용되는 MD5 key를 정의한다.
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
경계 라우터 보안기술
라우팅 테이블 보호 하기
라우팅 테이블 무결성
공격자는 보호되지 않은 라우터로 거짓 라우팅 update 패킷을 보내 라우팅 테이블에 오류를 발생하게 할 수 있다.
라우팅 테이블 무결성을 보호하기위한 방법
Static Route 만을 사용한다. Click
Route table update를 인증한다. Click
Passive interface를 사용한다.
네트워크의 다른 라우터가 동적으로 경로를 알아내는 것을 막기 위해 interface를 passive 상태로 만든다.
router(config)#key-string
상대방 라우터와 교환되는 message digest 또는 hash를 생성하는데 사용되는 MD5 key를 정의한다.
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
라우터 관리
Logging
security level
Cisco IOS 메시지는 severity level에 의해 분류된다.
Level 번호가 낮을 수록 중요한 메시지다.
Level | Name | Description
0 | Emergencies | Router unusable
1 | Alerts | Immediate action required
2 | Critical | Condition is critical
3 | Errors | Error condition
4 | Warnings | Warning condition
5 | Notifications | Normal but important event
6 | Informational | Informational message
7 | Debugging | Debug message
라우터가 기록하는 event
*System error
*라우터 설정 변경과 reboot
*Interface와 네트워크 상태 변경
*Login 실패
*Access list를 위반하는 traffic의 발생빈도
*라우터 암호화 보안 위반
Cisco 라우터 메시지에 포함되는 3가지 내용
Oct 29 10:00:01 EST: %SYS-5-CONFIG_I: Configured from console by vty0 (16.2.2.6)
완료
인터넷

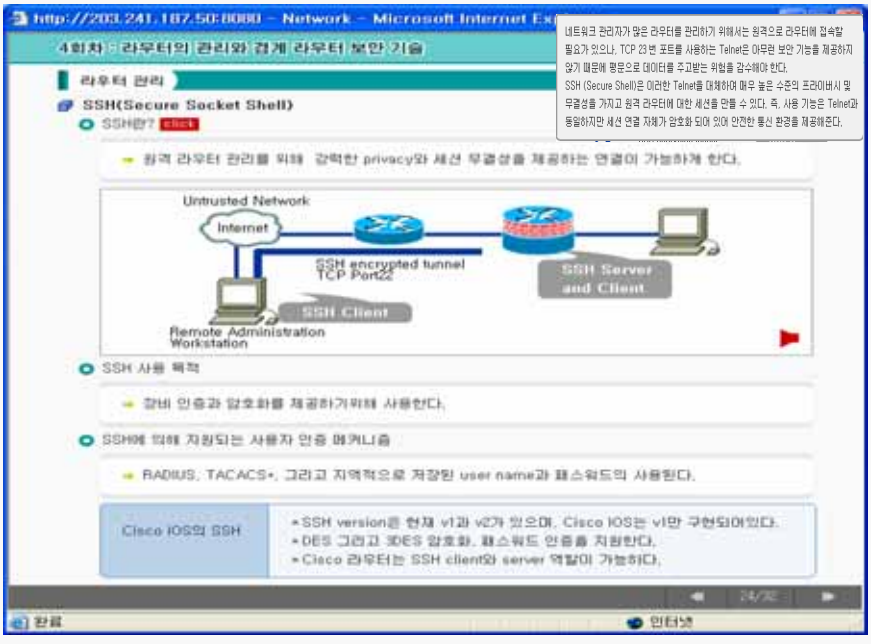

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 겹계 라우터 보안 기술
라우터 관리
Logging
Console logging
Router(config-if)#logging console info
access list log messages를 포함하는 모든 no
Router(config-if)#logging console debug
console상에 메시지를 보여준다.
Router(config-if)#logging console critical
console logging level을 2로 설정한다.
R2# config t
R2(config)# ! set console logging to level 5 (notify)
R2(config)# logging console notification
R2(config)# logging on
R2(config)# exit
Console level을 5로 또는 중요한 메시지는 console 상에 나타나지만 access list log 메시지는 나타나지않도록 하는 notification을 설정한다.
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.
완료
인터넷

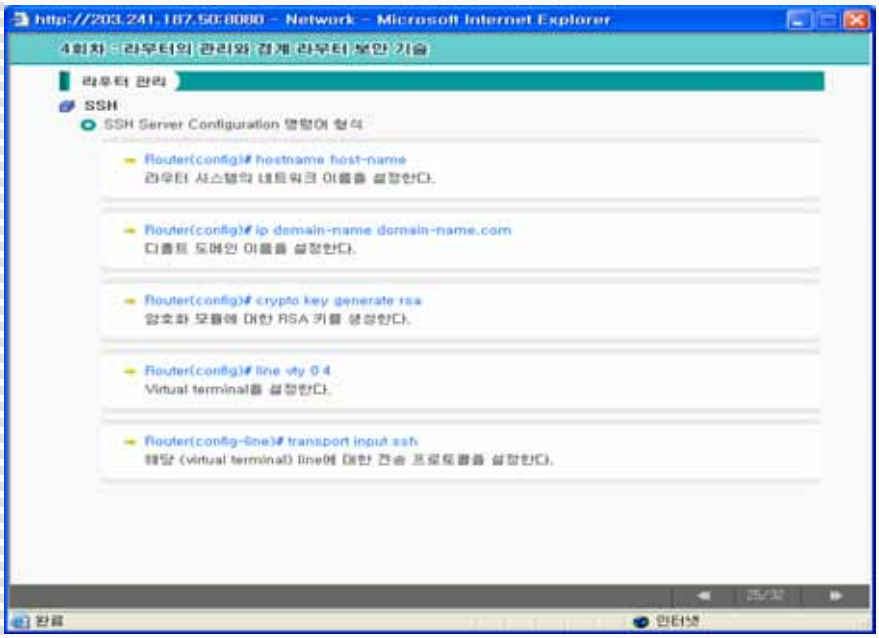

http://203.241.187.50:8080 - Network - Microsoft Internet Ex
4회차 : 라우터의 관리와 겹계 라우터 보안 기술
라우터 관리
Logging
Buffered logging
R2# config t
R2(config)# logging buffered 16000 information
R2(config)# service timestamp log data msec
local show-timezo
R2(config)# exit
R2# show logging
Buffered logging과 time stamp를 가능하게 하고 buffed log를 본다.
Terminal line logging
터미널 또는 가상 터미널은 log 모니터로 활용할 수 있다.
터미널 모니터 logging을 설정하기 위한 2가지 부분은 다음과 같다.
터미널 line 모니터 log 메시지를 위한 level을 설정.
특정한 line을 사용하는 동안 모니터하기 위한 것을 선언.
R2# config t
R2(config)# ! set monitor logging level to level 6
R2(config)# logging monitor information
R2(config)# exit
R2# terminal monitor
R2# config t
R2(config)# interface eth 0/1
R2(config)# ! shutdown will log a message, level 5
R2(config)# shutdown
Telnet 세션 가상 터미널 line상에 level 6로 터미널 line 모니터링을 설정한다.
Cisco 라우터는 메모리 버퍼에 로그 메시지를 저장할 수 있다. 버퍼링된 데이터는 라우터 exec 또는 enabled exec 세션에서만 사용가능하고, 라우터를 부팅하면 지워진다.
이와 같은 buffered logging이 유용하긴 하지만 로그 정보에 대한 장시간의 보호 기능은 제공하지 않는다. 일반적으로 로그 버퍼 크기는 대략 16KB 정도로 설정하는 것이 바람직하다.
완료
인터넷

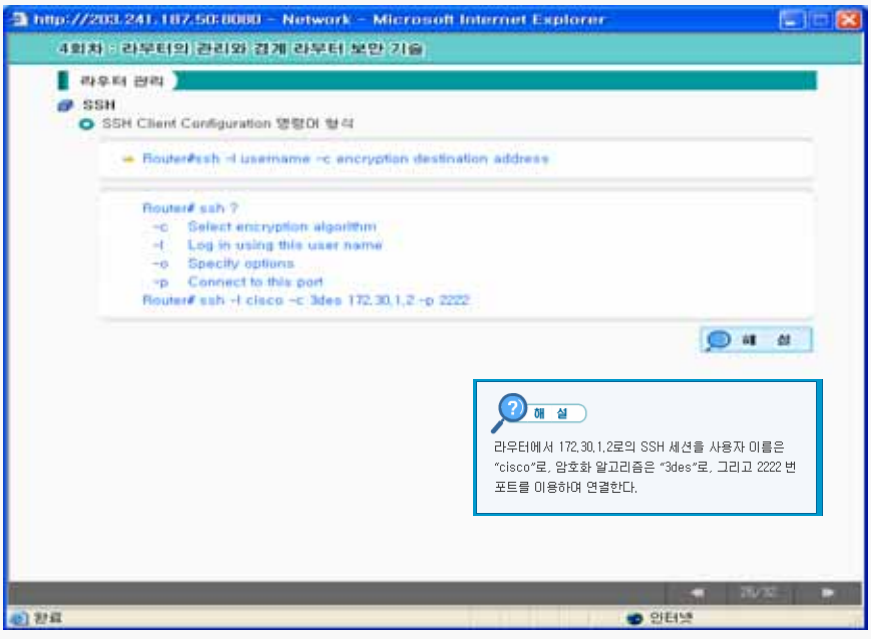

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 - 라우터의 관리와 경계 라우터 보안 기술
라우터 관리
Syslog logging
Syslog logging
Syslog Server
Syslog Client
ISP Router
172.30.0.0/24
Perimeter Router
Syslog client
10.0.0.0/24
Syslog server(destination host)
Student PC Syslog Server

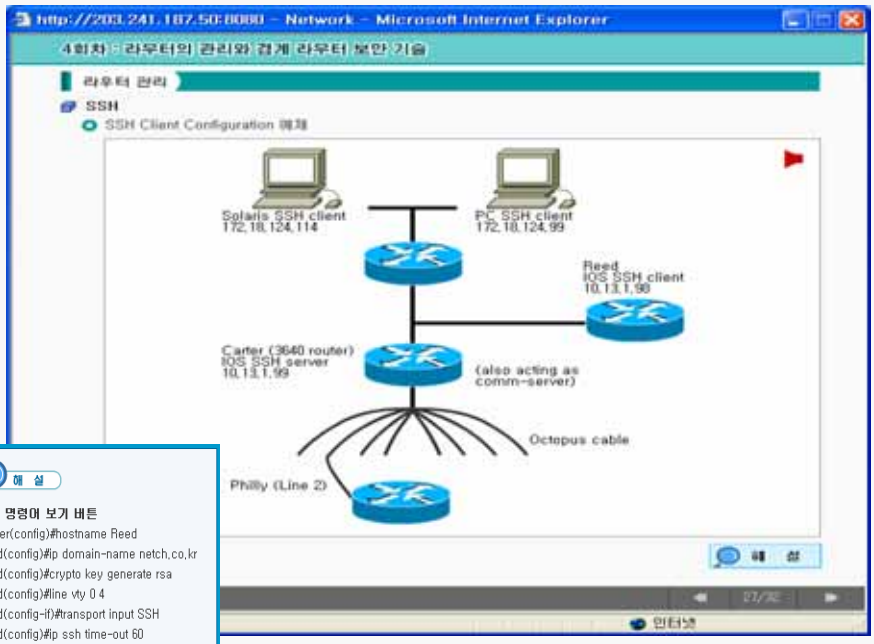

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 - 라우터의 관리와 경계 라우터 보안 기술
라우터 관리
Syslog logging
Syslog Router Commands
Router(config)#logging [host-name | ip-address]
Router(config)#logging trap level
Router(config)#logging facility facility-type
Router(config)#logging source-interface interface-type interface-number
Router(config)#logging on


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 - 라우터의 관리와 경계 라우터 보안 기술
라우터 관리
Time
Time의 중요성
정확한 시간은 완전한 네트워크 감사와 관리를 위해 중요하다.
네트워크 장비가 정확한 시간을 갖도록 하기 위한 방법
Network Time Protocol (NTP)
GPS
Two-Way Satellite
Modem Time Service
NTP
NTP는 네트워크에 존재하는 라우터들과 서버를 그리고 다른 장비들을 위한 일치된 시간 속
(time base)을 제공하여 장비들간의 시간을 동기화 하기 위해서 사용된다.
동기화된 time 시스템은 전자서명, 그리고 syslog 데이터 내의 이벤트의 올바른 해석을
위해 중요하다.
NTP는 UDP와 TCP 연결을 위해 포트 123를 사용한다.
NTP 설정 명령어 예
(config)# ntp authenticate
(config)# ntp authentication-key key number md5
[WORD | authentication key]
(config)# ntp trusted-key key number
(config)# ntp server [hostname | IP address of peer]
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Ex
4회차 - 라우터의 관리와 경계 라우터 보안 기술
네트워크 관리자가 많은 라우터를 관리하기 위해서는 원격으로 라우터에 접속할
필요가 있으나, TCP 23번 포트를 사용하는 Telnet은 아무런 보안 기능을 제공하지
않기 때문에 평문으로 데이터를 주고받는 위험을 감수해야 한다.
SSH (Secure Shell)은 이러한 Telnet을 대체하여 매우 높은 수준의 프라이버시 및
무결성을 가지고 원격 라우터에 대한 세션을 만들 수 있다. 즉, 사용 기능은 Telnet과
동일하지만 세션 연결 자체가 암호화 되어 있어 안전한 통신 환경을 제공해준다.
라우터 관리
SSH(Secure Socket Shell)
SSH란? click
원격 라우터 관리를 위해 강력한 privacy와 세션 무결성을 제공하는 연결이 가능하게 한다.
Untrusted Network
Internet
SSH encrypted tunnel
TCP Port22
SSH Server
and Client
SSH Client
Remote Administration
Workstation
SSH 사용 목적
장비 인증과 암호화를 제공하기위해 사용한다.
SSH에 의해 지원되는 사용자 인증 메커니즘
RADIUS, TACACS+, 그리고 지역적으로 저장된 user name과 패스워드의 사용된다.
Cisco IOS의 SSH
• SSH version은 현재 v1과 v2가 있으며, Cisco IOS는 v1만 구현되어있다.
• DES 그리고 3DES 암호화, 패스워드 인증을 지원한다.
• Cisco 라우터는 SSH client와 server 역할이 가능하다.
완료
인터넷

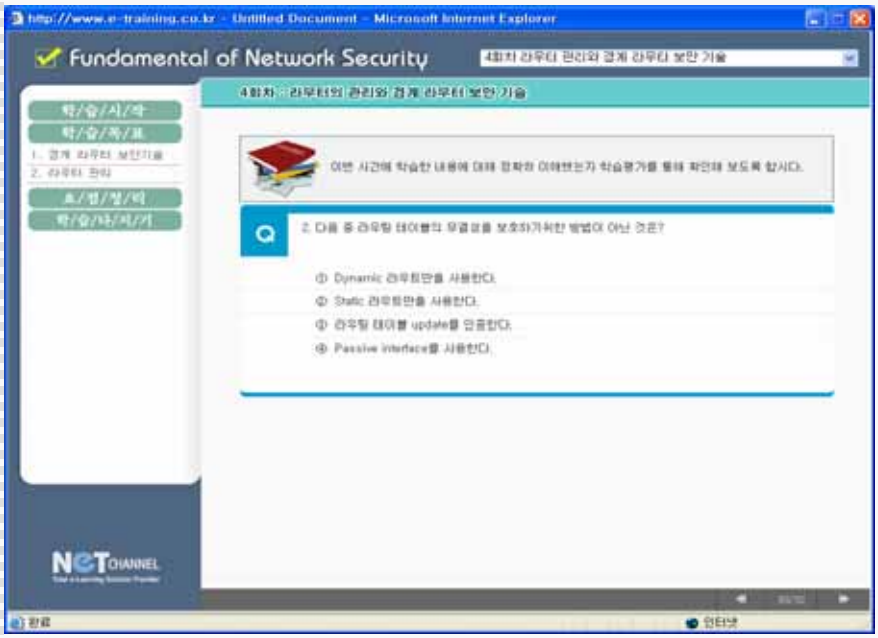

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 - 라우터의 관리와 경계 라우터 보안 기술
라우터 관리
SSH
SSH Server Configuration 명령어 형식
Router(config)# hostname host-name
라우터 시스템의 네트워크 이름을 설정한다.
Router(config)# ip domain-name domain-name.com
디폴트 도메인 이름을 설정한다.
Router(config)# crypto key generate rsa
암호화 모듈에 대한 RSA 키를 생성한다.
Router(config)# line vty 0 4
Virtual terminal을 설정한다.
Router(config-line)# transport input ssh
해당 (virtual terminal) line에 대한 전송 프로토콜을 설정한다.
완료
인터넷

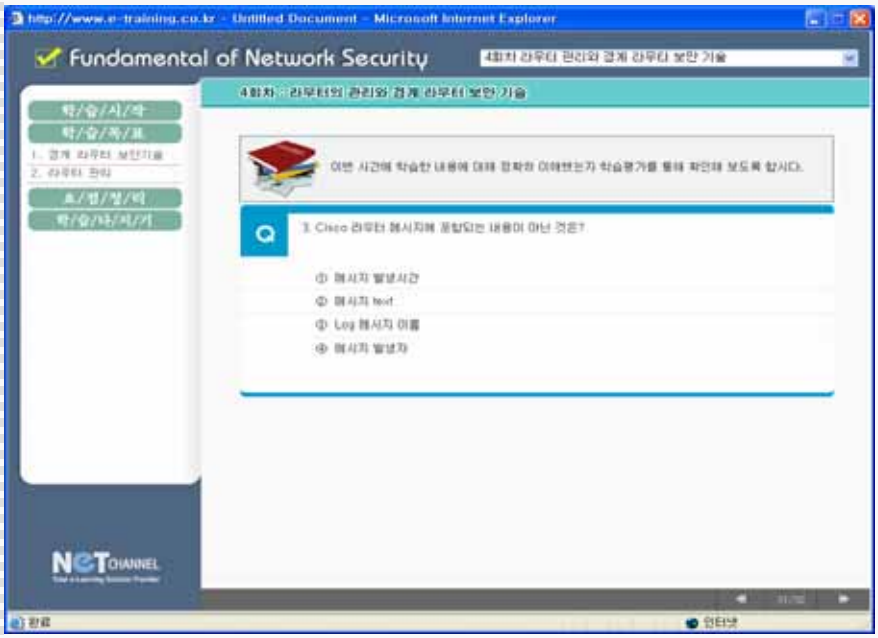

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 - 라우터의 관리와 경계 라우터 보안 기술
라우터 관리
SSH
SSH Client Configuration 명령어 형식
Router#ssh -l username -c encryption destination address
Router# ssh ?
-c Select encryption algorithm
-l Log in using this user name
-o Specify options
-p Connect to this port
Router# ssh -l cisco -c 3des 172.30.1.2 -p 2222
해 설
해 설
라우터에서 172.30.1.2로의 SSH 세션을 사용자 이름은 "cisco"로, 암호화 알고리즘은 "3des"로, 그리고 2222 번 포트를 이용하여 연결한다.
완료
인터넷

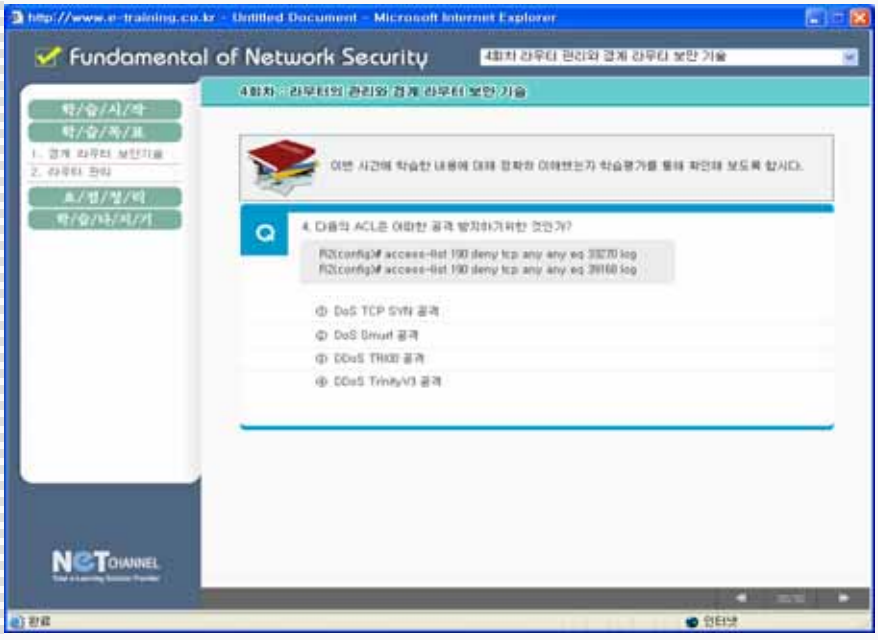

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 - 라우터의 관리와 경계 라우터 보안 기술
라우터 관리
SSH
SSH Client Configuration 예제
Solaris SSH client
172.18.124.114
PC SSH client
172.18.124.99
Reed
IOS SSH client
10.13.1.98
Carter (3640 router)
IOS SSH server
10.13.1.99
(also acting as comm-server)
Octopus cable
Philly (Line 2)
해 설
설정 명령어 보기 버튼
Router(config)#hostname Reed
Reed(config)#ip domain-name netch.co.kr
Reed(config)#crypto key generate rsa
Reed(config)#line vty 0 4
Reed(config-if)#transport input SSH
Reed(config)#ip ssh time-out 60
Reed(config)#ip ssh authentication-retries 2
Reed#ssh -l cisco -c des 10.13.1.99


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 - 라우터의 관리와 경계 라우터 보안 기술
지금까지 공부한 내용을 요약하여 다시 한번 정리를 하도록 하겠습니다.
부족한 부분은 다시 한번 확인 하시기 바랍니다.
경계 라우터 보안기술
Inbound와 Outbound 트래픽을 필터링하는 것은 네트워크보안을 강대 시킬 수 있다.
NAT는 외부 공격자로부터 내부 네트워크의 구조를 알아내기 어렵도록 한다.
NAT는 static과 dynamic NAT가 있다.
라우팅 테이블의 무결성을 보호하기위한 방법으로 static Route 사용, Route update 안함,
Passive interface가 있다.
라우터 관리
라우터에서 발생하는 여러 가지 event들을 logging하는 것은 관리와 보안을 위해 필요하다.
Logging 방법은 Console logging, Buffered Logging, Terminal line logging이 있고 Syslog서버를
이용하는 방법이 있다.
네트워크상의 여러 장비 간의 시간 동기화도 관리해야 하는 요소이다.
라우터에 원격접속을 안전하게 하기 위하여 SSH를 사용한다.


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
4회차 : 라우터의 관리와 경계 라우터 보안 기술
이번 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합시다.
1. 다음 중 네트워크 장비들이 정확한 시간을 갖도록 하는 방법이 아닌 것은?
① GPS
② SSH
③ NTP
④ Tow-Way Satellite
다음 문제
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
4회차 라우터 관리와 경계 라우터 보안 기술
4회차 : 라우터의 관리와 경계 라우터 보안 기술
이번 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합시다.
2. 다음 중 라우팅 테이블의 무결성을 보호하기위한 방법이 아닌 것은?
① Dynamic 라우팅만을 사용한다.
② Static 라우팅만을 사용한다.
③ 라우팅 테이블 update를 인증한다.
④ Passive Interface를 사용한다.
NETCHANNEL
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
4회차 라우터 관리와 경계 라우터 보안 기술
학/습/시/작
학/습/목/표
1. 경계 라우터 보안기술
2. 라우터 관리
요/점/정/리
학/습/자/료/실
4회차 : 라우터의 관리와 경계 라우터 보안 기술
이번 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합시다.
Q
3. Cisco 라우터 메시지에 포함되는 내용이 아닌 것은?
① 메시지 발생시간
② 메시지 text
③ Log 메시지 이름
④ 메시지 발생자
NETCHANNEL
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
4회차 라우터 관리와 경계 라우터 보안 기술
학/습/시/작
학/습/목/표
1. 경계 라우터 보안기술
2. 라우터 관리
요/점/정/리
학/습/자/료/실
4회차 : 라우터의 관리와 경계 라우터 보안 기술
이번 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합시다.
Q
4. 다음의 ACL은 어떠한 공격 방지하기위한 것인가?
R2(config)# access-list 190 deny tcp any any eq 31337 log
R2(config)# access-list 190 deny tcp any any eq 39168 log
① DoS TCP SYN 공격
② DoS Smurf 공격
③ DDoS TRIN 공격
④ DDoS Trinity/V3 공격
NETCHANNEL
완료
인터넷

End of Lecture