2022년도 2과제 모의고사_0402

* 2022년도 지방기능경기대회 2과제의 예상 문제로, 다음 문제가 어떤 장비에 적용되어 나오더라도 해결할 수 있도록 명령어를 충분히 숙지해야 한다.

1. 선수유의사항

- 대소문자 구분
- 암호 : cyberSecu12#$
- **도면의 모든 장비의 호스트이름을 도면과 동일하게 변경하시오.**

2. IP 구성

- A-PC, A-SRV, B-PC의 DNS 주소는 B-SRV의 IP주소를 사용
- C-PC1~2, C-LT1~2의 DNS 주소는 C-SRV의 IP주소를 사용

Network	HOST	IP Address
192.168.10.0/25	A-PC	DHCP 192.168.10.100~.120
	A-SW	192.168.10.2
	A-RT [G0/1.10]	192.168.10.1
192.168.10.128/25	A-SRV	192.168.10.129
	A-RT [G0/1.20]	192.168.10.254
67.20.10.0/24	A-RT [G0/0]	67.20.10.2
	B-RT1 [G0/1]	67.20.10.3
	B-RT2 [G0/1]	67.20.10.4
67.20.11.0/30	B-RT1 [S0/0/0]	67.20.11.1
	M-RT [S0/3/0]	67.20.11.2
67.20.12.0/30	B-RT2 [S0/0/1]	67.20.12.1
	M-RT [S0/3/1]	67.20.12.2
67.20.13.0/28	M-RT [G0/0]	67.20.13.1
	C-ASA [G1/1]	67.20.13.2
67.20.14.0/29	M-RT [G0/1]	서브넷의 마지막 주소
	B-SRV	67.20.14.1
67.20.15.0/30	B-RT2 [G0/0]	67.20.15.1
	B-PC	67.20.15.2
10.0.0.0/28	C-SRV	10.0.0.2
	C-ASA [G1/2]	10.0.0.1
192.168.10.0/24	C-ASA [G1/3]	192.168.10.1
	C-PC	DHCP 192.168.10.100~.120
	C-PC2	192.168.10.192
	C-Wireless [0/0]	192.168.10.10
172.16.0.0/25	C-Wireless	172.16.0.1
	C-LT1	DHCP 172.16.0.50~100
	C-LT2	

3. A-RT 네트워크 설정

1) A-SRV에 A-PC를 위한 DHCP 서버를 구성(pool name: A-PC-DHCP)
: DNS 서버 주소는 B-SRV주소를 사용

2) A-RT 기초 설정
: 가능한 모든 암호는 MD5 암호화되어 저장되어야 하고, 불가능한 암호의 경우 인코딩되어 저장되어야 한다.
가) 배너설정(A-SW 스위치에도 동일한 설정)

```
**********************************************************
* Unauthorized access to this device is prohibited! *
**********************************************************
```

나) A-SW, A-RT => 콘솔에서 발생하는 로그가 A-SRV에 저장되어야 한다.
다) 이전에 사용하던 명령어를 20개까지 저장되어야 한다.
라) 암호 길이가 8글자 이상이 되어야 한다.
마) 장비에 잘못된 명령어의 입력으로 장비가 일시적으로 멈추지 않도록 한다.
바) 장비에 발생하는 **메시지(로그)**로 입력 중인 명령어가 끊기지 않도록 한다.
사) 플래시에 저장되어 있는 IOS 파일이 보이지 않도록 설정한다.
아) 다음 A-SW의 vlan 설정에 따른 Inter-VLAN을 설정한다.
자) 콘솔 및 원격접속 시 A-SRV에 라디우스 인증을 받도록 한다.(인증키: radius123, 계정명 : **cyberAdmin**)
- 라디우스 인증 이용이 불가능할 경우 로컬계정(**localAdmin**)으로 로그인되어야 한다.
- localAdmin 로그인 시 바로 프리빌리지드 모드로 진입되어야 한다.
- 원격접속을 위한 ssh 설정(version 2)
  도메인(cyber.com), 키길이(1024)
  접속가능IP(192.168.10.100~.101)만 접속되도록 access-list 10을 사용하여 설정하시오.

차) 프리빌리지드 접속을 위한 암호를 설정하시오.
카) 사설 IP주소는 외부와의 통신 시 NAT(PAT)를 통해 통신되도록 하시오. 이때, access-list 20번을 사용

3) A-SW 설정
가) VLAN
vlan 10 (cyber) , fa0/1 ~ fa0/6
vlan 20 (dmz), fa0/10 ~ fa0/15
vlan 99 (secure), 위 포트를 제외한 모든 포트. native vlan

나) 트렁크
생성된 vlan 정보만 전송되어야 한다.
다) vlan 10에 소속된 포트는 spanning tree protocol(STP)를 비활성화해라

라) fa0/1, fa0/10 : 지금 연결된 호스트만 사용할 수 있어야 한다.
다른 호스트 연결시 동작 : fa0/1(통신불가능, 포트상태 유지), fa0/10(통신불가능, 포트상태 다운)

마) 원격접속이 ssh로 접속되도록 설정(version 2)
도메인(cyber.com), 키길이(1024)
접속계정 : sshAdmin
접속가능IP(192.168.10.100~.101)만 접속되도록 access-list 10을 사용하여 설정하시오.

4. M-RT 네트워크 설정

ssh(version 2) : 메인(cyber.com), 키길이(1024) , 계정(admin)

5. 라우팅 설정

1) OSPF 로 풀라우팅 한다.(사설네트워크는 제외한다.)

: process-id : 7, area 0 사용

: A-RT는 OSPF를 사용하지 않고, 아래와 같이 기본라우팅을 사용

2) 기본 라우팅

: A-RT는 기본라우팅(다음 홉 주소 사용)을 실시한다.

6. WAN 구간

1) clock rate : 1 Mbps => clock rate 10000000

2) PPP

- B-RT1/2 , M-RT 라우터의 WAN 인터페이스 구간에 대해 PPP/CHAP 로 보안 설정을 하시오.

3) 게이트웨이 이중화

- A-RT는 외부와 통신 시 B-RT1을 이용해야 한다. 만약, B-RT1에 문제가 발생하면 자동으로 B-RT2을 이용하여 통신하여야 한다. B-RT1이 문제에서 복구되면 B-RT2는 대기 상태가 되어야 한다.

- 이중화를 위한 게이트웨이 주소는 67.20.10.1를 사용하고, 그룹 번호는 2번을 사용한다.

7. 이더채널

- B-SW1~B-SW4 간에 LACP를 이용한 이더채널을 구성하시오.
- 이더채널 그룹

Group 1 : B-SW1 – B-SW2, B-SW3–B-SW4

Group 2 : B-SW2 – B-SW4

Group 3 : B-SW2 – B-SW3

8. B-SW2 스위치는 연결된 스위치에서 루트브릿지로 동작해야 한다.

9. 서버설정

1) A-SRV

가) 로그서버

- A-RT의 콘솔 로그가 저장되어야 한다.

나) 백업 서버

- A-SW의 현재 설정 파일을 TFTP를 이용하여 백업한다.
- A-SW-CONFIG.BAK

다) A-RT를 위한 라디우스 서버를 설정합니다.

2) B-SRV

가) DNS 서버

- **cybersecu.co.kr** --> B-SRV 주소

나) NTP 서버

- 모든 라우터들의 시간을 동기화 하시오.
- 인증키값은 1234, 암호는 기본암호를 사용

3) C-SRV

가) 라디우스 서버

- C-Wireless의 무선을 이용하는 클라이언트의 라디우스 서비스를 제공한다.
- 계정과 인증키는 “11.무선설정” 부분을 참고합니다.

나) 웹 : (intra.cyber.com)

다) DNS :

intra.cyber.com = 10.0.0.2 (C-SRV)

ex.cyber.com = 67.20.14.1 (B-SRV)

10. ASA 정책

enable 패스워드를 입력하시오.

1) 영역

가) Inside, g1/3 , security level 100

dhcp => C-PC를 위한 192.168.10.100~.120 /24

dns : 10.0.0.2

suffix : intra.cyber.com

나) DMZ, g1/2, security level 50

다) Outside, g1/1, security level 0

2) NAT (Inside -> Outside 통신 시)

nat 설정시 객체 이름 : In->Out-NAT

3) 방화벽 정책

가) Inside -> DMZ 허용 패킷

: icmp(C-PC2만 보낼 수 있도록), Radius, www, dns

: 정책이름 In->DMZ-permit

나) Inside -> Outside 허용 패킷

: B-SRV와의 웹서비스

: icmp (M-RT)

: 정책이름 In->Out-permit

4) 방화벽 ssh

- 계정 : **admin**
- 암호길이 1024 (도메인 : cyber.com)
- 접속가능한 IP주소 : 192.168.10.192~199

11. 무선 설정

1) 무선 연결 시 WPA2 Enterprise/AES를 이용한 C-SRV의 라디우스 인증을 실시한다.

2) 무선 설정 시 IP주소 목록에 있는 IP주소를 자동으로 받아와서 외부 네트워크와 연결되어야 한다.

- SSID : cyberW
- radius 인증 : Auth123 (계정 cyberUser / cyberP@ss123)
- 무선 연결시 IP 주소의 범위 172.16.0.50 ~ 172.16.0.100 , DNS 주소는 C-SRV 주소를 받아와야 한다.

12. Sniffer 설정

- C-SRV로 향하는 DNS, WWW, RADIUS, ICMP를 캡쳐하시오.

13. CBAC

외부에서 어떤 패킷도 들어올 수 없음

내부에서 외부로 나갔다가 되돌아오는 패킷 중 일부 허용하도록 설정

1) 정책 설정

- 외부에서 들어오는 모든 패킷을 차단(되돌아오는 패킷은 허용)
- 설정을 위해 access-list (name : out->in-deny)

2) 되돌아오는 허용 패킷

- 허용될 패킷 목록 : 웹, icmp (name : in->out-permit)