

2022년도 지방기능경기대회 채점기준(2과제)

1. 채점 시 유의사항	직 종 명	사이버 보안
<p>1. 선수가 제출한 비번호.pka 파일로 채점을 한다.</p> <p>2. 자동 채점은 파일을 열고 4~5분의 시간이 흘렀을 때, 완성도를 기준으로 한다.</p> <p>3. 4~5분은 도면 상의 시간을 의미하며, Fast Forward Time 으로 시간 조정이 가능하다.</p> <p>4. 문제에서 주어지지 않은 암호는 cyberSecu12#\$를 사용하며, 암호는 모두 md5 로 암호화 되어 저장되어야 한다.</p> <p>5. 방화벽 ASA의 경우 패킷트레이서 8.0 버전에서 파일을 열면 연결된 포트가 down 된 경우가 있을 수 있으므로, no shutdown을 하고 채점할 수 있다.</p> <p>6. 수동 채점 시 파일을 다시 열기, 장비를 다시 시작하기 등, 파일이나 장비를 다시 시작하는 것은 총 3회 이며, 재 부팅 시 발생하는 문제는 선수가 책임져야 한다.</p> <p>7. 제출된 파일에 문제가 있는 경우, 선수가 제출한 USB 속의 파일을 기준으로 다시 복사하여 채점할 수 있다. 어떠한 경우에도 선수 PC에 있는 파일로 채점하지 아니한다.</p>		

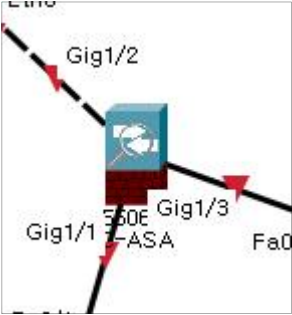
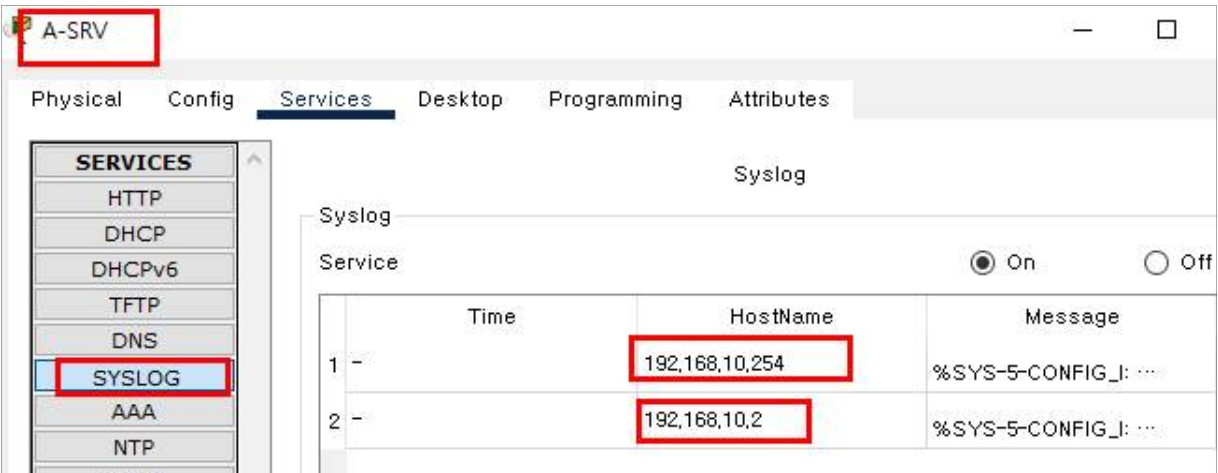
2. 채점기준표

1) 주요항목별 배점			직 종 명		사이버보안			
과제 번호	일련 번호	주요항목	배점	채점방법		채점시기		비고
				독립	합의	경기 진행중	경기 종료후	
제2과제	1	토폴로지 구성	30		○		○	
	2-1	배너 및 로그	0.2		○		○	
	2-2		0.3		○		○	
	3	무선 AAA 인증	1.0		○		○	
	4	라우터 라디우스인증	0.5		○		○	
	5	라우터 방화벽보안정책	2.0		○		○	
	6	라우팅	0.5		○		○	
	7	방화벽 DHCP	0.5		○		○	
	8-1	방화벽 정책	2.0		○		○	
	8-2		2.0		○		○	
	9	방화벽 SSH	0.7		○		○	
	10	Sniffer	0.3		○		○	
합 계			40					

2) 채점방법 및 기준(경기종료 후 채점)

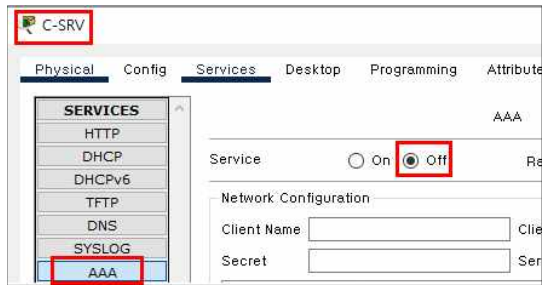
과제 번호	주요항목	일련 번호	세부항목(채점방법)	배점
제2과제	토폴로지 구성	1	완성도 × 0.3	30
	배너 및 로그	2-1	A-SW, A-RT의 배너확인	0.2
		2-2	A-SW, A-RT의 로그 확인	0.3
	무선 AAA 인증	3	C-Wireless 무선 설정	1.0
	라우터 라디우스인증	4	A-RT AAA 인증	0.5
	라우터 방화벽보안정책	5	A-RT 라우터 보안 정책	2.0
	라우팅	6	디폴트, OSPF 라우팅 설정	0.5
	방화벽 DHCP	7	ASA Inside dhcp 동작 확인	0.5
	방화벽 정책	8-1	DMZ 접근 정책 확인	2.0
		8-2	Outside 정책확인	2.0
	방화벽 SSH	9	ASA SSH 접근 정책 확인	0.7
	Sniffer	10	패킷캡처	0.3
합계				40

나. 채점방법 및 기준 (경기종료 후 채점)

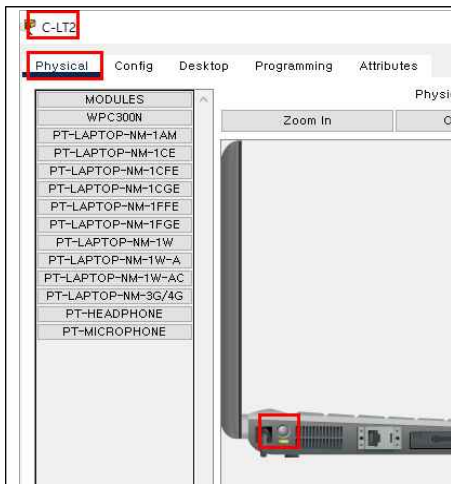
번호	세부 채점 내용
1	<p>1. 완성도 x 0.3 예) $100\% \times 0.3 = 30\text{점}$, $89\% \times 0.3 = 26.7\text{점}$</p> <p>채점 준비</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>패킷트레이서 이슈로 C-ASA 의 링크가 빨간색 링크일 경우 우측 명령어를 실행 후 수동 채점을 시작한다.</p>  </div> <div style="width: 50%;"> <pre> C-ASA>en Password: 암호(cyberSecu12#\$) C-ASA#conf t C-ASA(config)#int g1/1 C-ASA(config-if)#no shut C-ASA(config-if)#int g1/2 C-ASA(config-if)#no shut C-ASA(config-if)#int g1/3 C-ASA(config-if)#no shut </pre> </div> </div>
2	<p>2-1) 배너채점 0.2점 A-SW, A-RT 에 CLI 모드 접근시 다음 메시지가 정확히 보여야 함</p> <pre> ***** * Unauthorized access to this device is prohibited! * ***** </pre> <p>2-2) SYSLOG 확인 0.3점 A-SRV에서 다음과 같이 로그를 확인합니다. 192.168.10.254 , 192.168.10.2 에 대한 로그가 1개 이상이 존재해야 한다.</p> 

3. C-Wireless 설정 확인 - 1점 (모두 만족해야 정답으로 인정한다.)

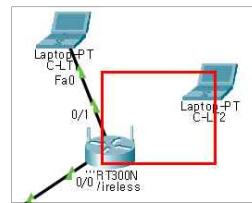
1) C-SRV의 라디우스 서비스를 off 한다.



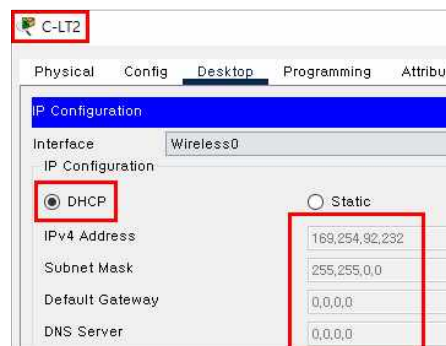
2) C-LT2 를 아래와 같이 재부팅 후 무선 연결이 안 되어야 하고, IP주소를 받아오지 않아야 한다.



다음과 같이 무선 연결이 되지 않아야 하며,



다음과 같이 실패한 IP주소를 받아야와야 한다.



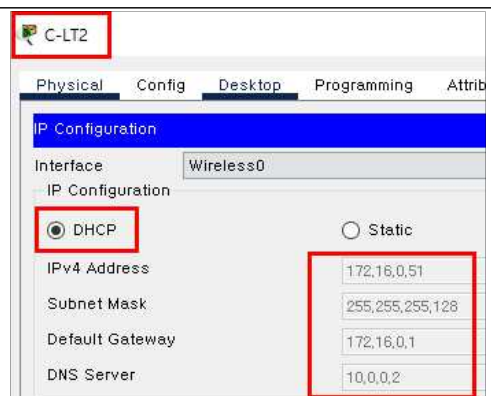
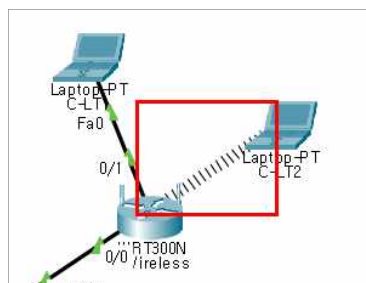
3 패킷트레이서 좌측 하단에 있는 다음 버튼 (Fast Forward Time)을 한번 클릭한다.



3) C-SRV의 AAA 서비스를 ON 한다.

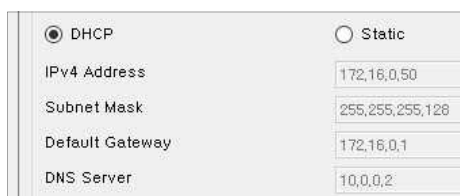
4) Time: 01:04:15 [Fast Forward Time] 를 한번 누르고 다음과 같이 C-LT2 의 IP가 자동으로 받아 한다.

다음과 같이 무선 연결이 자동으로 되어야 한다.



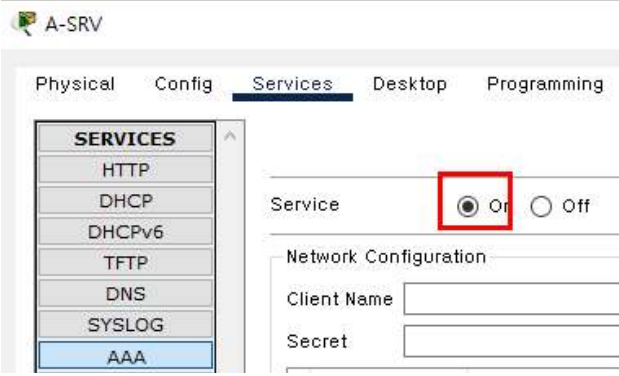
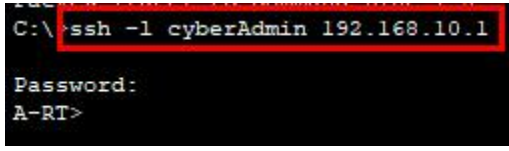
IP 주소의 범위 172.16.0.50 ~ 172.16.0.100

C-LT1 의 IP 구성이 다음과 같아야 한다. IP주소 범위(.50 ~ .100)



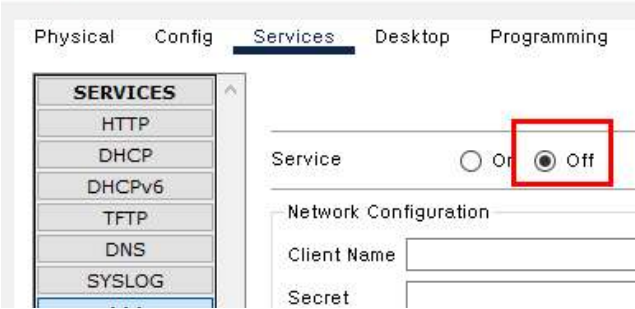
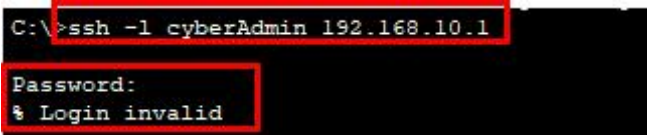
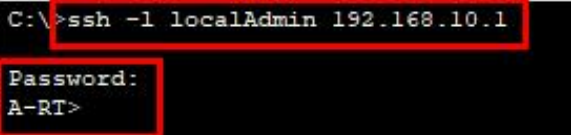
4. AAA 인증방식 - 0.5점

- 1) A-PC , A-RT 와 A-SRV에서 채점을 진행한다.
- 2) 라디우스 계정으로 로그인 성공하는지 확인한다.
(암호 cyberSecu12#\$)

	<p>A-RT에서 라디우스 계정으로 CLI 접속을 한다.</p> <p>Username: cyberAdmin Password:</p> <p>A-RT> exit 를 입력하여 연결을 끊는다.</p> <p>A-PC에서 진행 => 성공해야 한다.</p>  <p>로그인에 성공 후 exit 로 접속 해제한다.</p>
--	--

4

- 3) A-SRV 서버에 AAA 서비스를 이용하지 못할 경우, 로컬계정으로 로그인이 성공되어야 한다.
암호(cyberSecu12#\$) 을 정확히 입력해야 한다.

	<p>① A-RT 의 CLI에서 진행</p> <p>Username: cyberAdmin Password:</p> <p>% Login invalid (로그인이 실패해야 한다)</p> <p>Username: localAdmin Password:</p> <p>A-RT> (로그인이 성공해야 한다)</p>
<p>② A-PC에서 cyberAdmin 으로 실패해야 한다.</p>  <p>3번 실패</p>	<p>③ localAdmin 으로 성공해야 한다.,</p>  <p>A-SRV의 AAA를 다시 ON 한다.</p>

5. A-RT 보안 정책 - 2점

① A-RT에서 cyberAdmin으로 콘솔 로그인

//접속 불가능시 localAdmin 으로 시도한다.

Username: **cyberAdmin**

Password: **암호는 cyberSecu12#\$**

A-RT>en

Password: **암호는 cyberSecu12#\$**

A-RT#

② A-PC에 웹 접속 후, A-RT의 보안 이벤트를 확인



③ A-RT에서 다음과 같이 HTTP, UDP 에 대한 보안 로그가 보여야 한다.

A-RT#sh ip inspect sessions

Established Sessions

Session 803010216 (67.20.10.2:8)=>(67.20.10.4:0) icmp SIS_OPENING

Session 812604384 (67.20.10.2:1026)=>(67.20.14.1:80) http SIS_OPEN

Session 812601248 (67.20.10.2:1026)=>(67.20.14.1:53) udp SIS_OPEN

Session 513144680 (67.20.10.2:123)=>(67.20.14.1:123) udp SIS_OPEN

④ A-PC의 명령 프롬프트에서 B-SRV까지 경로를 확인한 후, A-RT의 보안 이벤트를 확인한다.

```
C:\>tracert 67.20.14.1

Tracing route to 67.20.14.1 over a maximum of 30 hops:
  0  0 ms    0 ms    0 ms   192.168.10.1
  1  0 ms    0 ms    0 ms   67.20.10.3
  2  0 ms    1 ms    0 ms   67.20.11.2
  3  1 ms    1 ms    1 ms   67.20.14.1
Trace complete.
```

⑤ 다음과 같이 icmp 보안 로그가 보여야 한다.(IP주소는 동일해야 하며, 포트번호는 다른 수 있음)

A-RT#sh ip inspect sessions

Established Sessions

Session 762762720 (67.20.10.2:8)=>(67.20.10.3:0) icmp SIS_OPENING

Session 762763896 (67.20.10.2:8)=>(67.20.10.4:0) icmp SIS_OPENING

Session 762763112 (67.20.10.2:8)=>(67.20.14.1:4) icmp SIS_OPEN

Session 513144680 (67.20.10.2:123)=>(67.20.14.1:123) udp SIS_OPEN

⑥ 다른 서비스는 차단되는지 확인한다.

- A-PC에서 B-SRV의 ftp 접속은 다음과 같이 불가능해야 한다.

```
C:\>ftp 67.20.14.1
Trying to connect...67.20.14.1
%Error opening ftp://67.20.14.1/ (Timed out)
```

⑦ B-PC에서 다음과 같이 FTP 접속이 가능해야 한다.

```
B-PC
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ftp 67.20.14.1
Trying to connect...67.20.14.1
Connected to 67.20.14.1
220- Welcome to PT Ftp server
Username:
```


6. 라우팅 - 0.5점

1) A-RT 의 라우팅 테이블이 다음과 같아야 한다.

A-RT#sh ip route

<생략>

```

67.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    67.20.10.0/24 is directly connected, GigabitEthernet0/0
L    67.20.10.2/32 is directly connected, GigabitEthernet0/0
192.168.10.0/24 is variably subnetted, 4 subnets, 2 masks
C    192.168.10.0/25 is directly connected, GigabitEthernet0/1.10
L    192.168.10.1/32 is directly connected, GigabitEthernet0/1.10
C    192.168.10.128/25 is directly connected, GigabitEthernet0/1.20
L    192.168.10.254/32 is directly connected, GigabitEthernet0/1.20
S*   0.0.0.0/0 [1/0] via 67.20.10.1

```

6

2) M-RT 의 라우팅 테이블은 다음과 같아야 한다. (단 업데이트 시간은 다른 수 있음)

사설IP 및 다른 네트워크가 O(ospf) 등 동적 라우트로 보이면 안 된다.

O가 표시된 경로와 직접 연결된 경로(C, L) 외 다른 라우팅 프로토콜(S, S*, R, D 등) 이 보이면 오답

M-RT# sh ip route

<생략>

```

67.0.0.0/8 is variably subnetted, 12 subnets, 5 masks
O    67.20.10.0/24 [110/65] via 67.20.11.1, 00:23:59, Serial0/3/0
      [110/65] via 67.20.12.1, 00:23:59, Serial0/3/1
C    67.20.11.0/30 is directly connected, Serial0/3/0
C    67.20.11.1/32 is directly connected, Serial0/3/0
L    67.20.11.2/32 is directly connected, Serial0/3/0
C    67.20.12.0/30 is directly connected, Serial0/3/1
C    67.20.12.1/32 is directly connected, Serial0/3/1
L    67.20.12.2/32 is directly connected, Serial0/3/1
C    67.20.13.0/28 is directly connected, GigabitEthernet0/0
L    67.20.13.1/32 is directly connected, GigabitEthernet0/0
C    67.20.14.0/29 is directly connected, GigabitEthernet0/1
L    67.20.14.6/32 is directly connected, GigabitEthernet0/1
O    67.20.15.0/30 [110/65] via 67.20.12.1, 00:4294967291:4294967242, Serial0/3/1

```

7. ASA DHCP 구성 - 0.5점

C-PC 에서 네트워크 구성 확인

C-PC

Physical Config Desktop Programming Attributes

Command Prompt

Packet Tracer PC Command Line 1.0

C:\>ipconfig /all

FastEthernet0 Connection:(default port)

```

Connection-specific DNS Suffix...: intra.cyber.com
Physical Address.....: 0006.2A77.7BEB
Link-local IPv6 Address.....: FE80::206:2AFF:FE7
IPv6 Address.....: ::
IPv4 Address.....: 192.168.10.100
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                        192.168.10.1
DHCP Servers.....: 192.168.10.1
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-5B-22-
DNS Servers.....: ::
                        10.0.0.2

```

7

8-1 DMZ 정책 확인 2점

1) ping 10.0.0.2 확인

C-PC = 실패	C-PC2 = 성공
<pre>C:\>ping 10.0.0.2 Pinging 10.0.0.2 with 32 bytes of data: Request timed out. Request timed out.</pre>	<pre>C:\>ping 10.0.0.2 Pinging 10.0.0.2 with 32 bytes of data: Reply from 10.0.0.2: bytes=32 time=1ms TTL=64 Reply from 10.0.0.2: bytes=32 time=1ms TTL=64</pre>

2) C-LT1 에서 다음과 같이 nslookup 이 성공해야 한다.

<pre>C:\>nslookup intra.cyber.com Server: [10.0.0.2] Address: 10.0.0.2 Non-authoritative answer: Name: intra.cyber.com Address: 10.0.0.2</pre>	<pre>C:\>nslookup ex.cyber.com Server: [10.0.0.2] Address: 10.0.0.2 Non-authoritative answer: Name: ex.cyber.com Address: 67.20.14.1</pre>
---	---

3) C-PC2에서 DMZ로 FTP 실패, 웹접속 성공

<p>C-PC2 에서 ftp 실패 확인</p> <pre>C:\>ftp 10.0.0.2 Trying to connect...10.0.0.2 %Error opening ftp://10.0.0.2/</pre>	<p>10.0.0.2 에 대해 웹 접속 성공</p> 
--	--

8

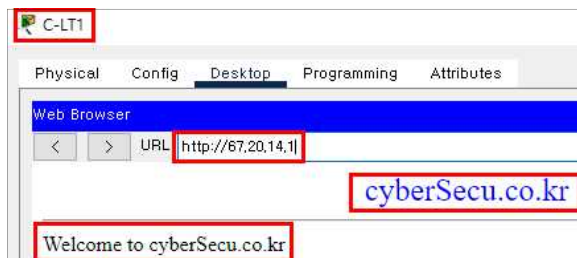
8-2 외부(Outside) 정책 확인 2점

1) ICMP 정책

C-PC2 에서 ping 확인 => 다음과 같아야한다. (67.20.13.1 만 성공해야한다)

<pre>C:\>ping 67.20.13.1 Pinging 67.20.13.1 with 32 bytes of data: Request timed out. Reply from 67.20.13.1: bytes=32 time=1ms TTL=64 Reply from 67.20.13.1: bytes=32 time=1ms TTL=64</pre>	<pre>C:\>ping 67.20.14.1 Pinging 67.20.14.1 with 32 bytes of data: Request timed out. Request timed out.</pre>	<pre>C:\>ping 67.20.15.2 Pinging 67.20.15.2 with 32 bytes of data: Request timed out. Request timed out.</pre>
--	---	---

2) 웹접속 성공



3) ftp 및 ssh 서비스 확인

C-PC에서 확인 = 실패 되어야 한다.

<pre>C:\>ftp 67.20.14.1 Trying to connect...67.20.14.1 %Error opening ftp://67.20.14.1</pre>	<pre>C:\>ssh -l admin 67.20.13.1 % Connection refused by remote host C:\></pre>
---	---

	<p>B-PC에서 확인 = 성공해야 한다.</p> <div> <div> C:\>ftp 67.20.14.1 Trying to connect...67.20.14.1 Connected to 67.20.14.1 220- Welcome to PT Ftp server Username: </div> <div> C:\>ssh -l admin 67.20.13.1 Password: </div> </div>
9	<p>9. ASA ssh 접속확인 0.7점</p> <div> <div> C-PC에서 접속 불가 </div> <div> C-PC2에서 접속 성공 </div> </div>
10	<p>10. Sniffer - 정책 확인 0.3점</p> <p>채점기준표 공개로 답이 공개될 수 있는 항목이므로 비공개</p>