

DevSecOps를 활용한 클라우드 보안 전문가 양성 과정

네트워크 서버 구축 과정 평가 제출

-정재호-

서술형 평가

- 1.1 OSI 7 Layer의 계층 순서에 대해 서술하고 /24 서브넷마스크 값에서 최소 3개의 서브네트워크로 분할할 때의 서브넷마스크 값을 입력하시오.

OSI 7 Layer 순서 : 물리 > 데이터 링크 > 네트워크 > 전송 > 세션 > 표현 > 애플리케이션

서브넷마스크 값 : /26 , 255.255.255.192, 와일드카드(0.0.0.63)

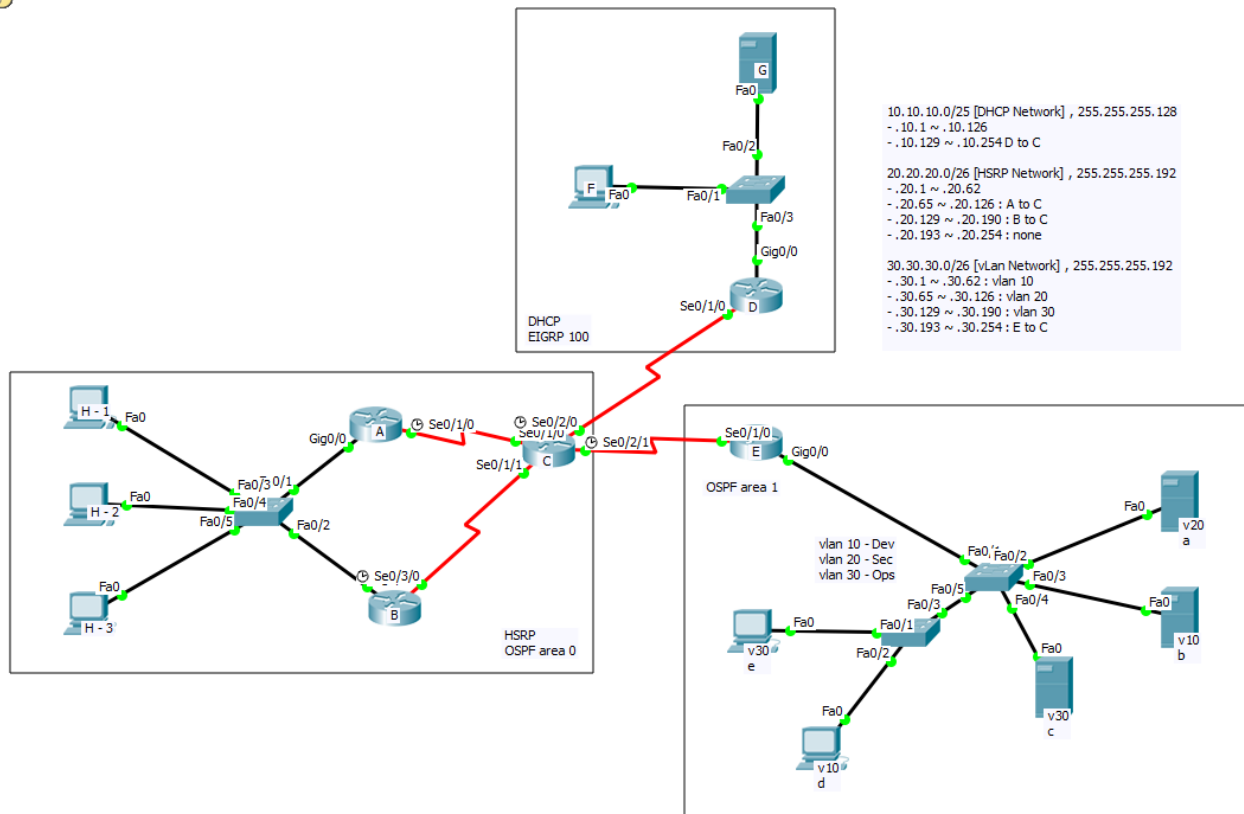
- 2.1 서버(Server)와 클라이언트(Client)의 개념에 대해 서술하시오.

서버 (Server)	클라이언트(Client)로 받은 요청을 처리하고 결과를 클라이언트로 다시 전달하는 주체 서비스 관리를 위해 필요한 데이터를 DB에 저장하고 관리자가 확인할 수 있는 log 값 으로 표현하는 기능 수행
클라이언트 (Client)	서비스의 사용자 또는 서비스를 사용하기 위해 필요한 물리적 장치 사용자는 클라이언트를 인터페이스로서 사용 서버에 기능을 요청하고 결과를 받아 다시 사용자에게 제공하는 역할 수행

과제 평가

1.2 ~ 1.4 Packet Tracer에 토폴로지를 작성한 후 주소 및 라우팅 설정을 통해 전체 노드 간 통신이 가능하게 설정하고 세부 조건에 따라 기술을 설정하고 확인하시오.

IP / 라우팅 결과 토폴로지



라우팅 테이블

- D 라우터 (EIGRP 100 라우팅)

```
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C    10.10.10.0/25 is directly connected, GigabitEthernet0/0
L    10.10.10.126/32 is directly connected, GigabitEthernet0/0
C    10.10.10.128/25 is directly connected, Serial0/1/0
L    10.10.10.129/32 is directly connected, Serial0/1/0
20.0.0.0/26 is subnetted, 3 subnets
D EX 20.20.20.0/26 [170/2681856] via 10.10.10.130, 00:19:19, Serial0/1/0
D EX 20.20.20.64/26 [170/2681856] via 10.10.10.130, 00:19:19, Serial0/1/0
D EX 20.20.20.128/26 [170/2681856] via 10.10.10.130, 00:19:19, Serial0/1/0
30.0.0.0/26 is subnetted, 4 subnets
D EX 30.30.30.0/26 [170/2681856] via 10.10.10.130, 00:19:19, Serial0/1/0
D EX 30.30.30.64/26 [170/2681856] via 10.10.10.130, 00:19:19, Serial0/1/0
D EX 30.30.30.128/26 [170/2681856] via 10.10.10.130, 00:19:19, Serial0/1/0
D EX 30.30.30.192/26 [170/2681856] via 10.10.10.130, 00:19:19, Serial0/1/0
```

- C 라우터 (OSPF area 0 라우팅, EIGRP 재분배)

```
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D    10.10.10.0/25 [90/2170112] via 10.10.10.129, 00:20:25, Serial0/2/0
C    10.10.10.128/25 is directly connected, Serial0/2/0
L    10.10.10.130/32 is directly connected, Serial0/2/0
20.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O    20.20.20.0/26 [110/65] via 20.20.20.65, 00:31:54, Serial0/1/0
      [110/65] via 20.20.20.129, 00:31:54, Serial0/1/1
C    20.20.20.64/26 is directly connected, Serial0/1/0
L    20.20.20.66/32 is directly connected, Serial0/1/0
C    20.20.20.128/26 is directly connected, Serial0/1/1
L    20.20.20.130/32 is directly connected, Serial0/1/1
30.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O    30.30.30.0/26 [110/65] via 30.30.30.193, 00:31:26, Serial0/2/1
O    30.30.30.64/26 [110/65] via 30.30.30.193, 00:31:26, Serial0/2/1
O    30.30.30.128/26 [110/65] via 30.30.30.193, 00:31:26, Serial0/2/1
C    30.30.30.192/26 is directly connected, Serial0/2/1
L    30.30.30.194/32 is directly connected, Serial0/2/1
```

- E 라우터 (OSPF area 1 라우팅)

```
10.0.0.0/25 is subnetted, 1 subnets
O E2 10.10.10.0/25 [110/20] via 30.30.30.194, 00:22:43, Serial0/1/0
20.0.0.0/26 is subnetted, 3 subnets
O IA 20.20.20.0/26 [110/129] via 30.30.30.194, 00:32:38, Serial0/1/0
O IA 20.20.20.64/26 [110/128] via 30.30.30.194, 00:32:38, Serial0/1/0
O IA 20.20.20.128/26 [110/128] via 30.30.30.194, 00:32:38, Serial0/1/0
30.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C    30.30.30.0/26 is directly connected, GigabitEthernet0/0.10
L    30.30.30.62/32 is directly connected, GigabitEthernet0/0.10
C    30.30.30.64/26 is directly connected, GigabitEthernet0/0.20
L    30.30.30.126/32 is directly connected, GigabitEthernet0/0.20
C    30.30.30.128/26 is directly connected, GigabitEthernet0/0.30
L    30.30.30.190/32 is directly connected, GigabitEthernet0/0.30
C    30.30.30.192/26 is directly connected, Serial0/1/0
L    30.30.30.193/32 is directly connected, Serial0/1/0
```

DHCP 설정 (라우터 D)

```
ip dhcp pool dhcp
network 10.10.10.0 255.255.255.128
default-router 10.10.10.126
dns-server 8.8.8.8
```

- DHCP 적용 결과

IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IP Address	10.10.10.2
Subnet Mask	255.255.255.128
Default Gateway	10.10.10.126
DNS Server	8.8.8.8

HSRP 설정 (라우터 A, B)

- 라우터 A (Active 라우터)

```
interface GigabitEthernet0/0
ip address 20.20.20.60 255.255.255.192
duplex auto
speed auto
standby version 2
standby 0 ip 20.20.20.62
standby preempt
standby 0 track Serial0/1/0
```

- 라우터 B (Standby 라우터)

```
interface GigabitEthernet0/0
ip address 20.20.20.61 255.255.255.192
duplex auto
speed auto
standby version 2
standby 0 ip 20.20.20.62
standby priority 95
standby preempt
standby 0 track Serial0/3/0
```

vLan 설정

- Server mode switch

VLAN	Name	Status	Ports
1	default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
10	Dev	active	Fa0/3
20	Sec	active	Fa0/2
30	Ops	active	Fa0/4
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- Client mode switch

VLAN	Name	Status	Ports
1	default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig0/1, Gig0/2
10	Dev	active	Fa0/2
20	Sec	active	
30	Ops	active	Fa0/1
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

ACL 설정

- ACL 설정 시나리오

C -> G : http x, ping o

그 외 시스템 접속 허용

H -> G: FTP x

그 외 트래픽 허용

- 해석

G 서버가 속한 10.10.10.0 네트워크는 DHCP 설정으로 인해 접속 IP가 유동적이다.

DHCP 설정을 수정해 특정 IP를 G 서버에 할당하거나,

10.10.10.0 네트워크 전체에 ACL 설정을 적용해 트래픽을 차단할 수 있다.

10.10.10.0 네트워크 전체에 HTTP, FTP 트래픽을 차단하는 시나리오로 작업 진행

- 설정 결과

```
access-list 100 deny tcp host 30.30.30.129 10.10.10.0 0.0.0.127 eq www
access-list 100 deny tcp 20.20.20.0 0.0.0.63 10.10.10.0 0.0.0.127 eq ftp
access-list 100 permit ip any any
```

위 두 설정을 통해 http, ftp 접속은 불가능하고,

그 외 트래픽은 'permit ip any any'를 통해 수신 가능해 진다.

2.1 ~ 2.2 Linux(Rocky 9) 및 Windows 2022 Server를 설치하고 구성도에 맞게 서버를 구축하고 테스트하여 결과를 확인하도록 하시오.

- IP 설정 변경 사항
- 테스트를 위해 아래와 같이 설정 값이 변경되었습니다.

설정	전	후
V10 Client(Host Windows 10)	30.30.30.2/26	192.168.1.8/16
V20 Server(WindowsServer 2022)	30.30.30.65/26	192.168.1.102/16
V10 Server(Linux Server 1)	30.30.30.1/26	192.168.1.110/16
V30 Server(Linux Server 2)	30.30.30.129/26	192.168.1.111/16

Gateway(192.168.0.1), DNS(192.168.1.110)으로 통일

Linux Server 1 설정

- NFS 서버/클라이언트 연결 여부 확인

```
root@Linux1:/nfs-server
TriggeredBy: ● rpcbind.socket
Docs: man:rpcbind(8)
Main PID: 6263 (rpcbind)
Tasks: 1 (limit: 11108)
Memory: 960.0K
CPU: 19ms
CGroup: /system.slice/rpcbind.service
└─6263 /usr/bin/rpcbind -w -f

Sep 02 13:48:18 Linux1 systemd[1]: Starting RPC Bind...
Sep 02 13:48:18 Linux1 systemd[1]: Started RPC Bind.
[root@Linux1 nfs-server]# vi /etc/exports
[root@Linux1 nfs-server]# vi /etc/exports
[root@Linux1 nfs-server]# rm /etc/exports
rm: remove regular file '/etc/exports'? y
[root@Linux1 nfs-server]# systemctl restart rpcbind
[root@Linux1 nfs-server]# systemctl status rpcbind
[root@Linux1 nfs-server]# ls -al
total 0
drwxrwxrwx. 2 root root 29 Sep 2 14:01
dr-xr-xr-x. 19 root root 253 Sep 2 13:36 ..
-rw-r--r--. 1 root root 0 Sep 2 14:01 nfsTestFile.txt
[root@Linux1 nfs-server]#
```

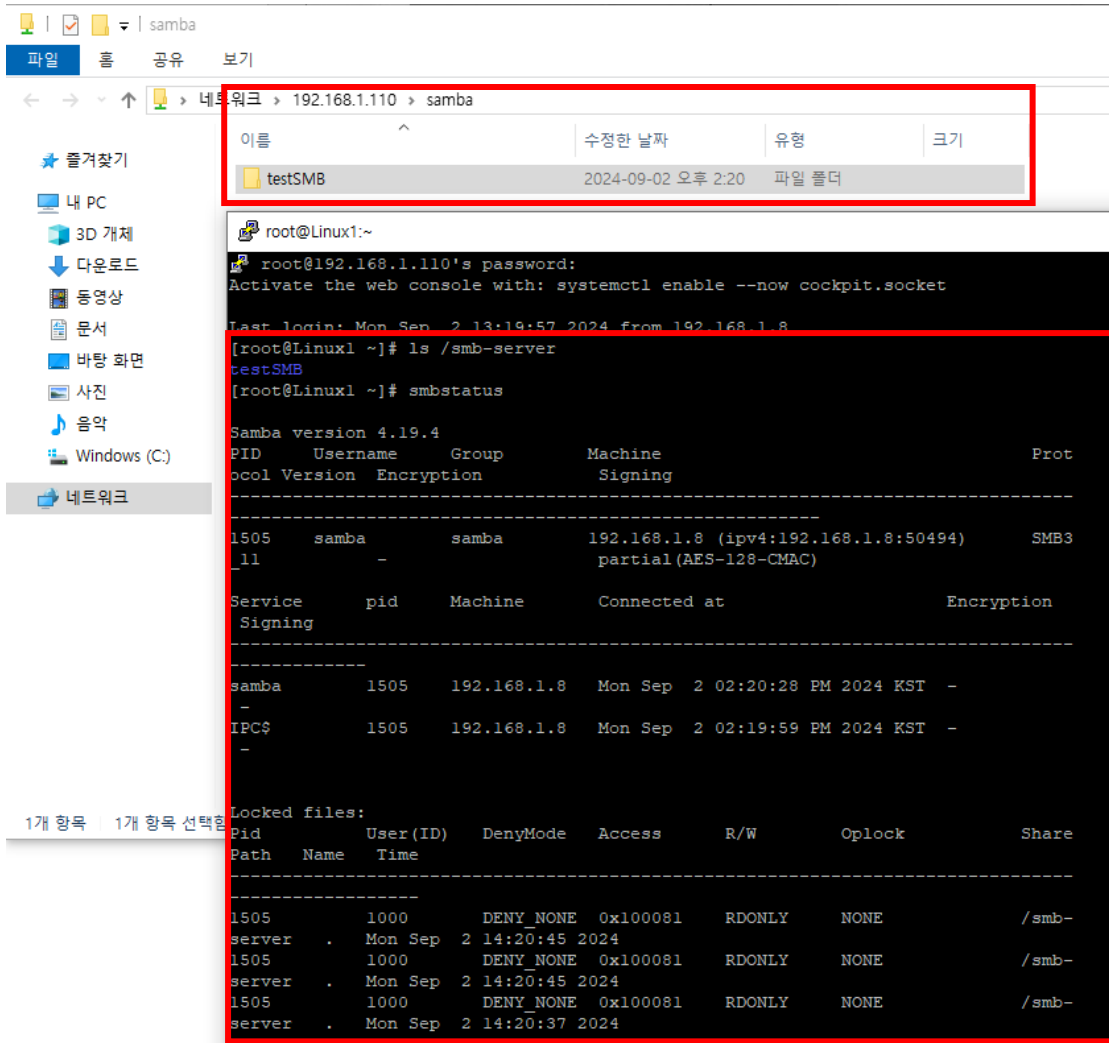
```
root@Linux2:~
ward, --remove-masquerade, --remove-icmp-block, --remove-icmp-block-inversion,
--remove-forward-port, --remove-entry, --remove-entries-from-file, --remove-dest
ination, --remove-module, --remove-helper, --remove-include, --remove-passthroug
h, --remove-chain, --remove-rule, --remove-rules
[root@Linux2 ~]# firewall-cmd --permanent --remove-service=nfs
success
[root@Linux2 ~]# firewall-cmd --permanent --add-port=2049/tcp
success
[root@Linux2 ~]# firewall-cmd --reload
success
[root@Linux2 ~]# mount -t nfs 192.168.1.110:/nfs-server /mnt
mount.nfs: access denied by server while mounting 192.168.1.110:/nfs-server
[root@Linux2 ~]# systemctl start rpcbind
[root@Linux2 ~]# systemctl enable rpcbind
Unknown command verb enable.
[root@Linux2 ~]# systemctl enable rpcbind
[root@Linux2 ~]# mount -t nfs 192.168.1.110:/nfs-server /mnt
[root@Linux2 ~]# touch /mnt/nfsTestFile.txt
[root@Linux2 ~]# ls -al /mnt/
total 0
drwxrwxrwx. 2 root root 29 Sep 2 14:01
dr-xr-xr-x. 18 root root 235 Aug 30 08:44 ..
-rw-r--r--. 1 root root 0 Sep 2 14:01 nfsTestFile.txt
[root@Linux2 ~]#
```

- DNS 설정

```
root@Linux1:~
$TTL      86400
@          IN      SOA      ns.hoje99.com.  root.hoje99.com. (
                        20240902
                        24H
                        15M
                        48H
                        86400)
;
ns         IN      NS       ns.hoje99.com.
ns         IN      A        192.168.1.110
nfs        IN      A        192.168.1.110
smb1       IN      A        192.168.1.110
logS       IN      A        192.168.1.110
https      IN      A        192.168.1.111
sftp       IN      A        192.168.1.111
smb2       IN      A        192.168.1.111
http       IN      A        192.168.1.110
```

(작동 확인)

- Samba 연결확인



The screenshot shows a Windows File Explorer window with the address bar set to '네트워크 > 192.168.1.110 > samba'. The left sidebar shows the '네트워크' (Network) location selected. The main pane displays a folder named 'testSMB' with a modification date of '2024-09-02 오후 2:20' and a type of '파일 폴더' (File Folder).

Below the file explorer, a terminal window shows the output of the following commands:

```

root@Linux1:~# ls /smb-server
testSMB
root@Linux1:~# smbstatus

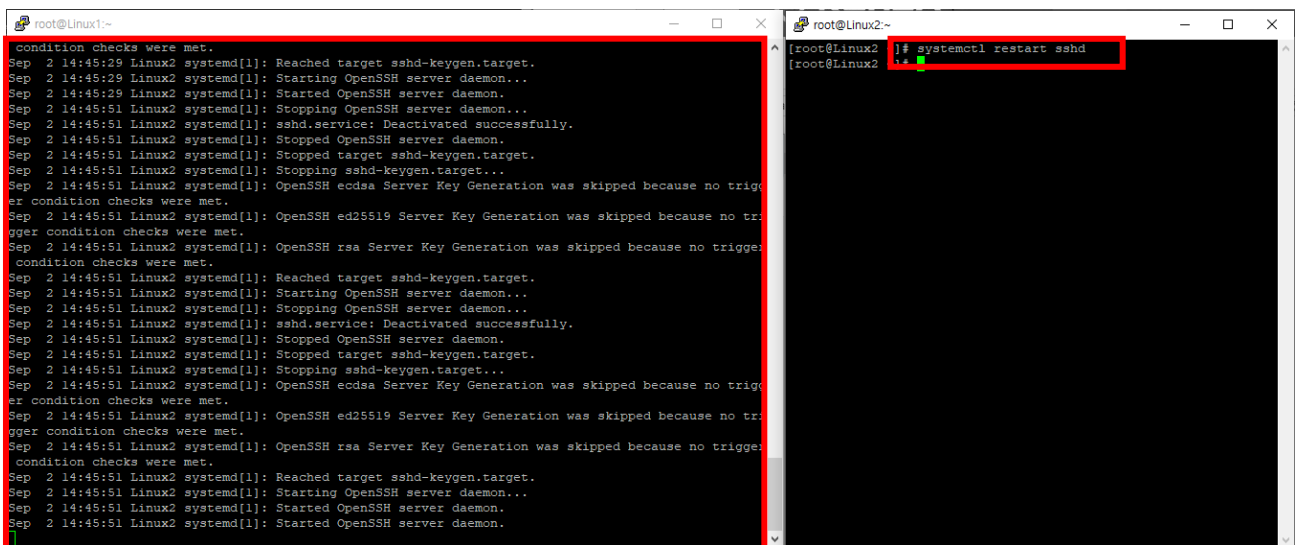
Samba version 4.19.4
PID Username Group Machine Prot
ocol Version Encryption Signing
-----
1505 samba samba 192.168.1.8 (ipv4:192.168.1.8:50494) SMB3
_ll - partial(AES-128-CMAC)

Service pid Machine Connected at Encryption
-----
samba 1505 192.168.1.8 Mon Sep 2 02:20:28 PM 2024 KST -
IPC$ 1505 192.168.1.8 Mon Sep 2 02:19:59 PM 2024 KST -

Locked files:
Pid User (ID) DenyMode Access R/W Oplock Share
Path Name Time
-----
1505 1000 DENY NONE 0x100081 RDONLY NONE /smb-
server . Mon Sep 2 14:20:45 2024
1505 1000 DENY NONE 0x100081 RDONLY NONE /smb-
server . Mon Sep 2 14:20:45 2024
1505 1000 DENY NONE 0x100081 RDONLY NONE /smb-
server . Mon Sep 2 14:20:37 2024

```

- Log 서버/클라이언트 동기화 확인



The screenshot shows two terminal windows. The left window, titled 'root@Linux1:~', shows the output of the 'systemctl restart sshd' command, which includes the following lines:

```

Sep 2 14:45:51 Linux2 systemd[1]: Reached target sshd-keygen.target.
Sep 2 14:45:51 Linux2 systemd[1]: Starting OpenSSH server daemon...
Sep 2 14:45:51 Linux2 systemd[1]: Started OpenSSH server daemon.
Sep 2 14:45:51 Linux2 systemd[1]: Stopping OpenSSH server daemon...
Sep 2 14:45:51 Linux2 systemd[1]: sshd.service: Deactivated successfully.
Sep 2 14:45:51 Linux2 systemd[1]: Stopped OpenSSH server daemon.
Sep 2 14:45:51 Linux2 systemd[1]: Stopped target sshd-keygen.target.
Sep 2 14:45:51 Linux2 systemd[1]: Stopping sshd-keygen.target...
Sep 2 14:45:51 Linux2 systemd[1]: OpenSSH ecdsa Server Key Generation was skipped because no trigger condition checks were met.
Sep 2 14:45:51 Linux2 systemd[1]: OpenSSH ed25519 Server Key Generation was skipped because no trigger condition checks were met.
Sep 2 14:45:51 Linux2 systemd[1]: OpenSSH rsa Server Key Generation was skipped because no trigger condition checks were met.
Sep 2 14:45:51 Linux2 systemd[1]: Reached target sshd-keygen.target.
Sep 2 14:45:51 Linux2 systemd[1]: Starting OpenSSH server daemon...
Sep 2 14:45:51 Linux2 systemd[1]: Started OpenSSH server daemon.
Sep 2 14:45:51 Linux2 systemd[1]: Stopping OpenSSH server daemon...
Sep 2 14:45:51 Linux2 systemd[1]: sshd.service: Deactivated successfully.
Sep 2 14:45:51 Linux2 systemd[1]: Stopped OpenSSH server daemon.
Sep 2 14:45:51 Linux2 systemd[1]: Stopped target sshd-keygen.target.
Sep 2 14:45:51 Linux2 systemd[1]: Stopping sshd-keygen.target...
Sep 2 14:45:51 Linux2 systemd[1]: OpenSSH ecdsa Server Key Generation was skipped because no trigger condition checks were met.
Sep 2 14:45:51 Linux2 systemd[1]: OpenSSH ed25519 Server Key Generation was skipped because no trigger condition checks were met.
Sep 2 14:45:51 Linux2 systemd[1]: OpenSSH rsa Server Key Generation was skipped because no trigger condition checks were met.
Sep 2 14:45:51 Linux2 systemd[1]: Reached target sshd-keygen.target.
Sep 2 14:45:51 Linux2 systemd[1]: Starting OpenSSH server daemon...
Sep 2 14:45:51 Linux2 systemd[1]: Started OpenSSH server daemon.

```

The right window, titled 'root@Linux2:~', shows the output of the 'systemctl restart sshd' command, which includes the following lines:

```

[root@Linux2 ~]# systemctl restart sshd
[root@Linux2 ~]#

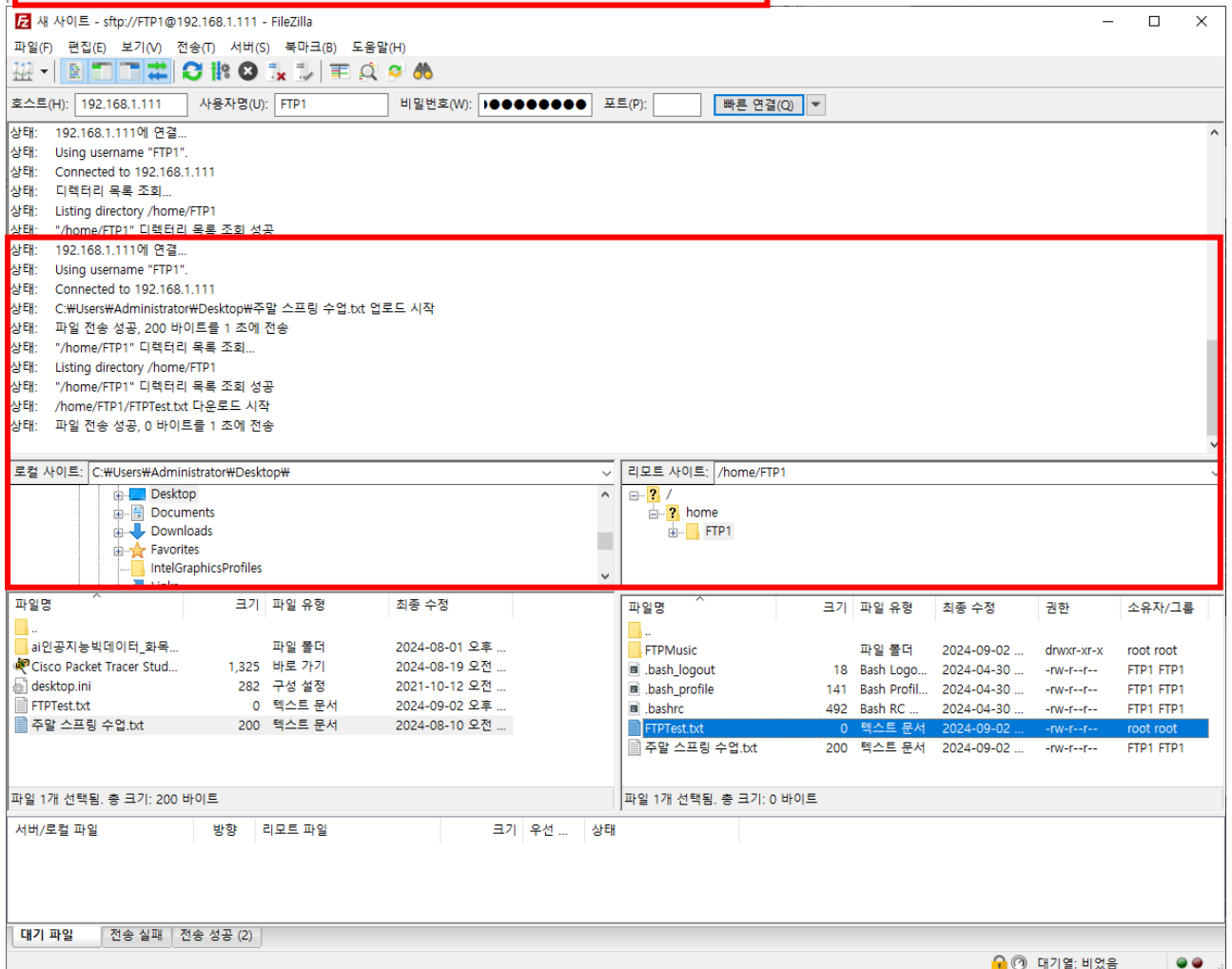
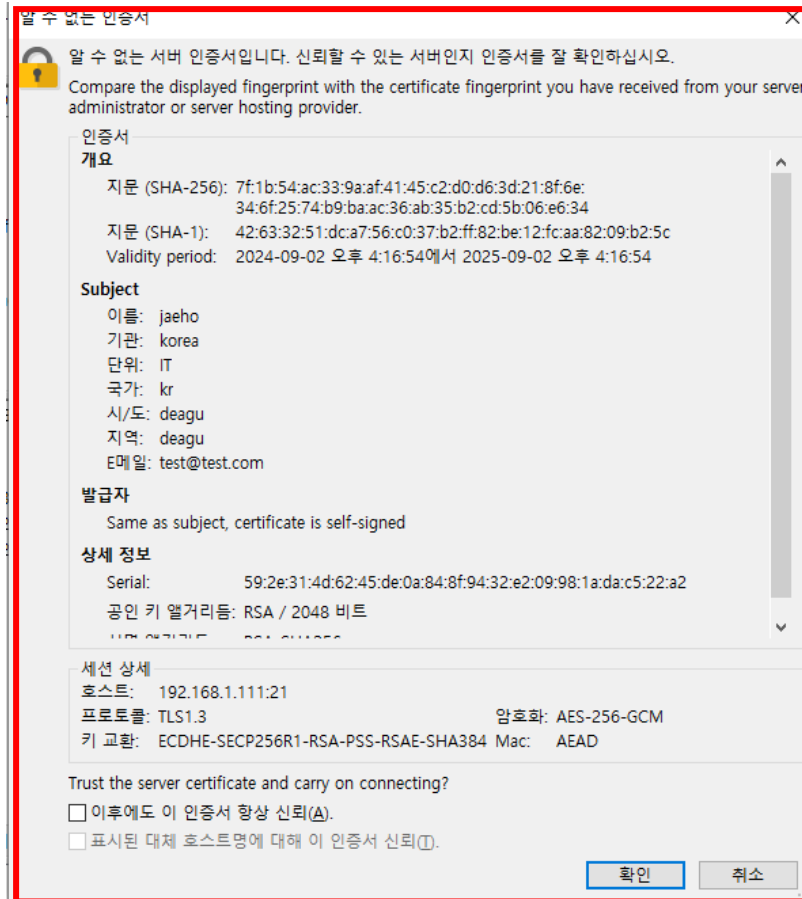
```

Linux Server 2 설정

- https 접속 확인



- sFTP 접속 확인



- samba server 연결 확인

The image displays a Windows File Explorer window and a Linux terminal window, both highlighting Samba server connection details.

Windows File Explorer (Network Location):

이름	수정된 날짜	유형	크기
새 폴더	2024-09-02 오후 4:29	파일 폴더	
새 폴더 (2)	2024-09-02 오후 4:29	파일 폴더	
새 폴더 (3)	2024-09-02 오후 4:29	파일 폴더	
새 폴더 (4)	2024-09-02 오후 4:29	파일 폴더	
test.txt	2024-09-02 오후 4:29	텍스트 문서	OKB

Linux Terminal Output:

```
[root@Linux2 ~]# smbstatus
```

PID	Username	Group	Machine	Protocol	Version	Encryption
2307	samba	samba	192.168.1.8 (ipv4:192.168.1.8:50975)	SMB3_11		-

```
Service pid Machine Connected at Encryption Signing
```

Service	pid	Machine	Connected at	Encryption	Signing
samba	2307	192.168.1.8	Mon Sep 2 04:29:04 PM 2024 KST	-	-

```
Locked files:
```

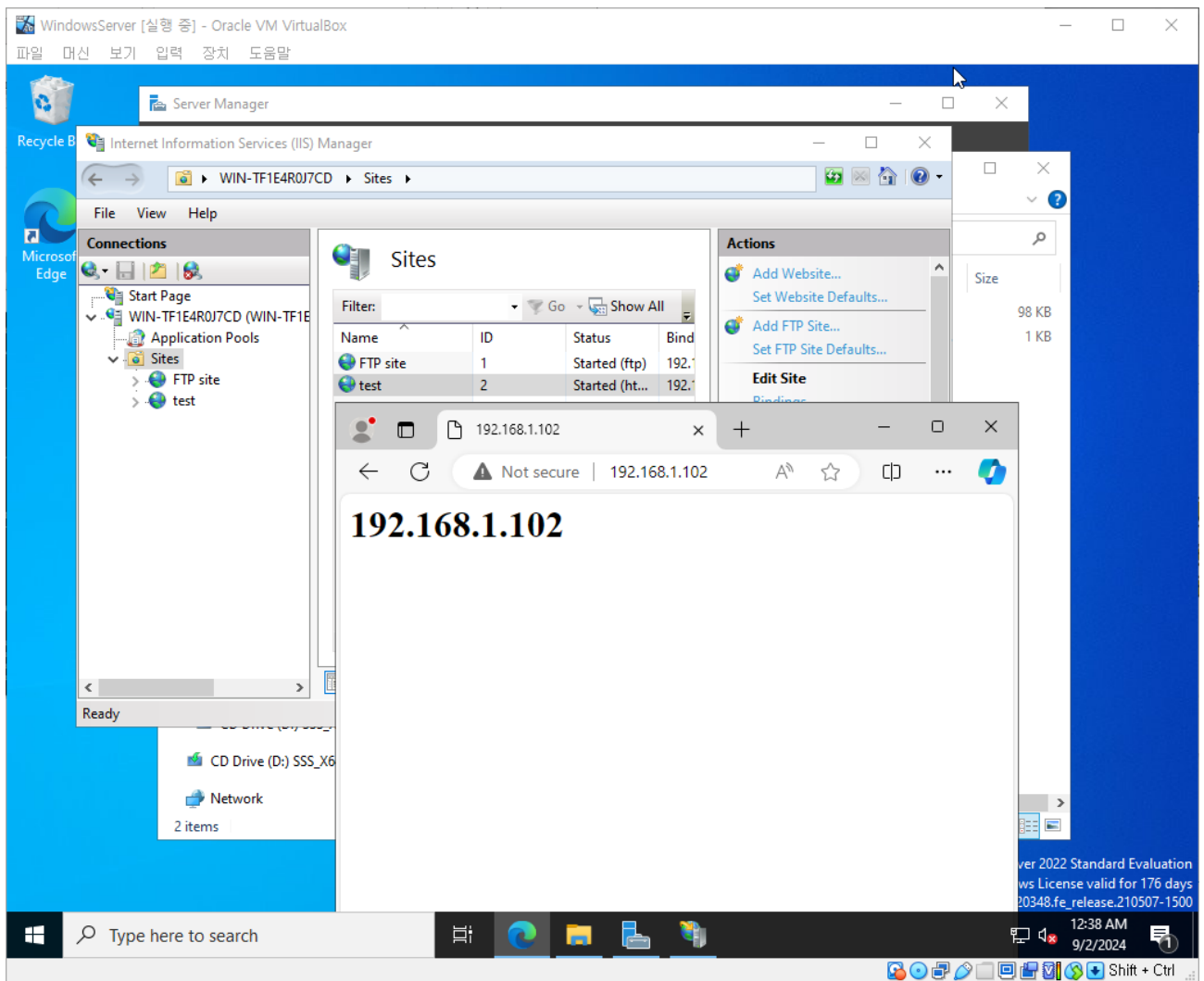
Pid	User(ID)	DenyMode	Access	R/W	Oplock	SharePath	Name	Time
2307	1001	DENY_NONE	0x100081	RDONLY	NONE	/smb-server	.	Mon Sep 2 16:29:28
2307	1001	DENY_NONE	0x100081	RDONLY	NONE	/smb-server	.	Mon Sep 2 16:29:28
2307	1001	DENY_NONE	0x100081	RDONLY	NONE	/smb-server	.	Mon Sep 2 16:29:15

```
[root@Linux2 ~]# ls -al /smb-server/
```

Permissions	Owner	Group	Size	Time	File
d-----w--w--	2 samba	samba	6	Sep 2 16:29	새 폴더
drwxrwxrwx	6 root	root	106	Sep 2 16:29	새 폴더 (2)
dr-xr-xr-x	19 root	root	273	Sep 2 16:24	..
d-----w--w--	2 samba	samba	6	Sep 2 16:29	새 폴더 (3)
d-----w--w--	2 samba	samba	6	Sep 2 16:29	새 폴더 (4)
-----w--w--	1 samba	samba	0	Sep 2 16:29	test.txt

Window Server 설정

- http Web Server



DNS 적용 확인

- host 장치의 DNS 주소를 192.168.1.110으로 변경 후 테스트

The screenshot displays the FileZilla interface with the following details:

- Host:** 192.168.1.111
- User:** FTP1
- Status Log:**
 - Connected to 192.168.1.111
 - C:\Users\Administrator\Desktop# 주말 스프링 수업.txt 업로드 시작
 - 파일 전송 성공, 200 바이트를 1 초에 전송
 - "/home/FTP1" 디렉터리 목록 조회...
 - Listing directory /home/FTP1
 - "/home/FTP1" 디렉터리 목록 조회 성공
 - /home/FTP1/FTPTest.txt 다운로드 시작
 - 파일 전송 성공, 0 바이트를 1 초에 전송
 - 서버와의 연결이 종료됨
 - 서버와의 연결이 종료됨
 - sftp.hoje99.com에 연결...
 - Using username "FTP1".
 - Connected to sftp.hoje99.com
 - 디렉터리 목록 조회...
 - Listing directory /home/FTP1
 - "/home/FTP1" 디렉터리 목록 조회 성공
- Local Site:** C:\Users\Administrator\Desktop#
- File List:**

파일명	크기	파일 유형	최종 수정
..		파일 폴더	2024-08-01 오전
ai인공지능빅데이터_화목...		파일 폴더	2024-08-19 오전
Cisco Packet Tracer Stud...	1,325	바로 가기	2021-10-12 오전
desktop.ini	282	구성 설정	2024-09-02 오전
FTPTest.txt	0	텍스트 문서	2024-08-10 오전
주말 스프링 수업.txt	200	텍스트 문서	2024-08-10 오전
- Summary:** 파일 1개 선택됨. 총 크기: 200 바이트
- Transfer:** 대기 파일, 전송 실패, 전송 성공 (2)

도메인 이름을 통한 원활한 연결 확인