

23장 프록시 서버와 방화벽

강사 김영석

A top-down view of a wooden desk. On the desk, there is a silver laptop with a black keyboard, a pair of black-rimmed glasses, a white coffee cup with a yellow handle, and a small green succulent in a pot. The word 'CONTENT' is written in large, white, sans-serif capital letters over the left side of the image.

CONTENT

- 1 프록시 서버의 개요
- 2 프록시 서버 구축 하기
- 3 방화벽의 개요
- 4 방화벽 설정 하기

1. 프록시 서버의 개요

- ❖프록시 서버란 클라이언트가 자신을 거쳐 다른 네트워크에 접속할 수 있도록 중간에서 대리해주는 서버를 말한다.
- ❖서버와 클라이언트 사이에 대리로 통신을 수행하는 것을 프록시라고 하고 그 기능을 하는 서버를 프록시 서버라 부른다.
- ❖외부에서 한번 가져온 데이터나 파일들을 프록시 서버에 캐시에 저장해 두었다가 다른 클라이언트가 캐시에 저장된 내용을 요청할 경우 외부로 가지 않고 캐시에서 주기 때문에 빠른 서비스가 가능하다는 장점이 있다.

2. 프록시 서버 구축 하기

❖ Squid 프록시 서버 설치하기

```
user1@Server1:~/바탕화면$ sudo apt-get install -y squid
[sudo] user1 암호:
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다... 완료
상태 정보를 읽는 중입니다... 완료
다음의 추가 패키지가 설치될 것입니다 :
  libcap3 squid-common squid-langpack
제안하는 패키지:
  squidclient squid-cgi squid-purge resolvconf smbclient winbind
```

```
user1@Server1:~/바탕화면$ systemctl status squid.service
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-08-29 16:38:54 KST; 37s ago
     Docs: man:squid(8)
  Process: 18994 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
 Main PID: 18997 (squid)
    Tasks: 4 (limit: 2132)
```


❖ IP 기반 인증 설정 하기

```
user1@Server1:~/바탕화면$ sudo vi /etc/squid/squid.conf
```

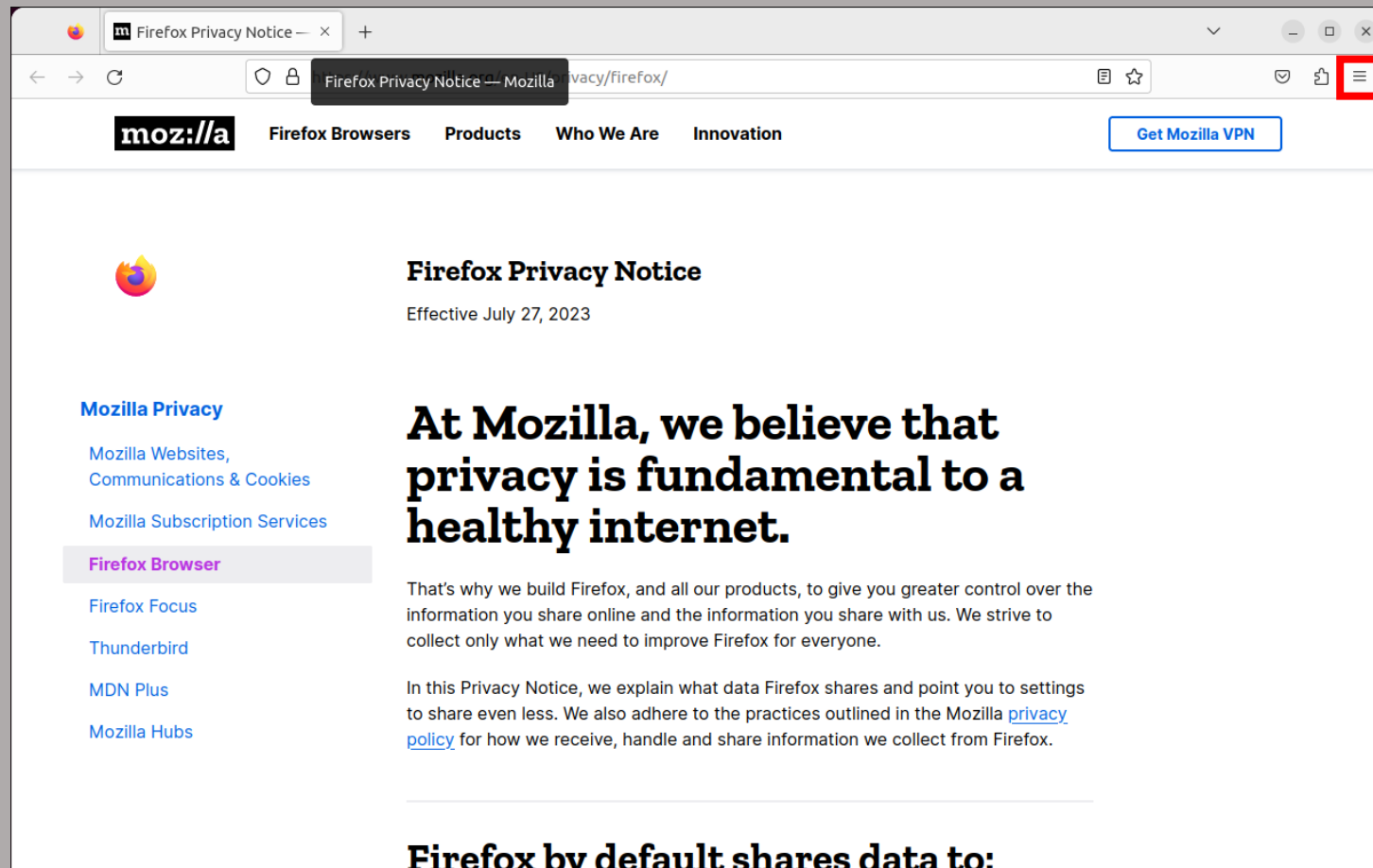
```
acl Server2 src 10.100.0.102
acl client_range src 10.100.0.0/255.255.255.0
http_access allow Server2 client_range
#       WELCOME TO SQUID 5.2
#       -----
#
#       This is the documentation for the Squid
#       This documentation shows what the defaults for various c
#       happen to be.  If you don't need to change the default,
:wq
```

```
user1@Server1:~/바탕화면$ sudo systemctl restart squid
```

```
user1@Server1:~/바탕화면$ sudo systemctl status squid
```

```
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-08-29 16:55:23 KST; 2s ago
     Docs: man:squid(8)
  Process: 19199 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
 Main PID: 19203 (squid)
    Tasks: 4 (limit: 2132)
```

❖ 클라이언트 설정하기



데이터 동기화 및 저장

로그인

새 탭Ctrl+T

새 창Ctrl+N

새 사생활 보호 창Ctrl+Shift+P

북마크>

기록>

다운로드Ctrl+Shift+Y

비밀번호

부가 기능 및 테마Ctrl+Shift+A

인쇄...Ctrl+P

페이지를 다른 이름으로 저장...Ctrl+S

페이지에서 찾기...Ctrl+F

확대/축소- 100 % + ↗

설정

기타 도구>

도움말>

종료Ctrl+Q

🔍 설정에서 찾기

⚙️ 일반

🏠 홈

🔍 검색

🔒 개인 정보 및 보안

🔄 Sync

Mozilla 추가 제품 정보

🔌 확장 기능 및 테마

❓ Firefox 도움말

탐색

☐ 자동 스크롤 사용(A)

☒ 부드러운 스크롤 사용(M)

☐ 항상 스크롤 막대 표시(O)

☐ 커서 키를 항상 페이지 내에서 사용(C)

☐ 입력을 시작할 때 텍스트 찾기(X)

☒ 화면 속 화면 비디오 컨트롤 사용(E) [더 알아보기](#)

☒ 키보드, 헤드셋 또는 가상 인터페이스를 통해 미디어 제어(V) [더 알아보기](#)

☒ 탐색할 때 확장 기능 추천(R) [더 알아보기](#)

☒ 탐색할 때 기능 추천(F) [더 알아보기](#)

네트워크 설정

Firefox가 인터넷에 접근하는 방법을 설정하세요. [더 알아보기](#)

설정...(E)

연결 설정



인터넷 프록시 접근 설정

- ☐ 프록시 사용 안 함(Y)
- ☐ 프록시 설정 자동 감지(W)
- ☐ 시스템 프록시 설정 사용(U)
- ☒ 수동 프록시 설정(M)

HTTP 프록시(X)

10.100.0.101

포트(P)

3128

☒ HTTPS에도 이 프록시를 사용

HTTPS 프록시

10.100.0.101

포트(O)

3128

SOCKS 호스트

포트(T)

0

☐ SOCKS v4 ☒ SOCKS v5

☐ 자동 프록시 설정 URL(A)

새로 고침(E)

프록시 사용 안 함(N):

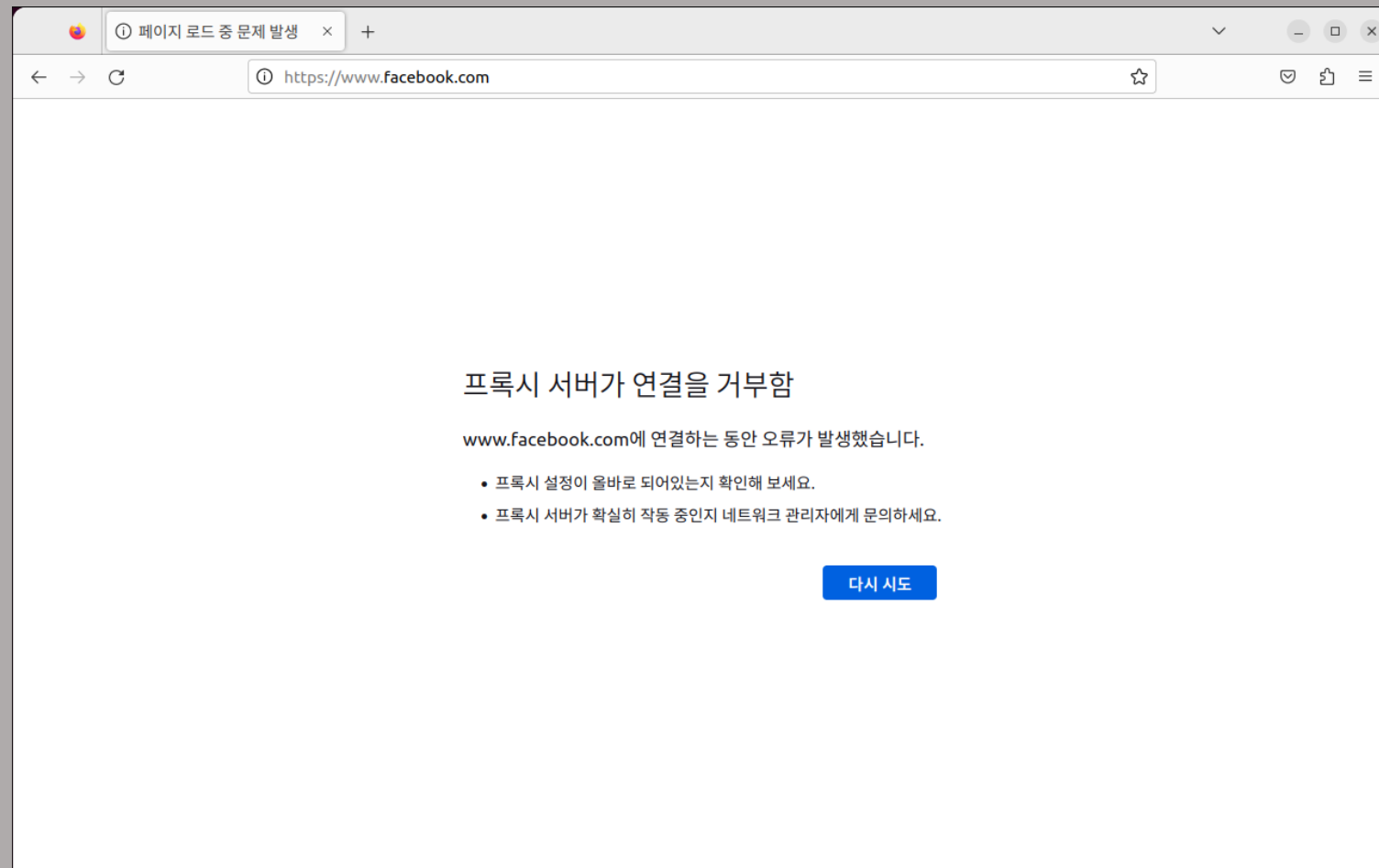
예: .mozilla.org, .net.nz, 192.168.1.0/24

취소

확인




```
user1@Server1:~/바탕화면$ sudo systemctl stop squid.service
```



❖ 사용자 기반 인증 설정하기

```
user1@Server1:~/바탕화면$ sudo htpasswd -c /etc/squid/passwd Server2
New password:
Re-type new password:
Adding password for user Server2
user1@Server1:~/바탕화면$ sudo htpasswd /etc/squid/passwd client_range
New password:
Re-type new password:
Adding password for user client_range
user1@Server1:~/바탕화면$ cat /etc/squid/passwd
Server2:$apr1$v0F7eUZP$c3mjNcYNH/DR20k6nsB.w1
client_range:$apr1$fyKtgohc$Nphy2s.g/MR9zenzRq.fT1
```



```
user1@Server1:~/바탕화면$ sudo vi /etc/squid/squid.conf
```

```
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwd
acl ncsa_users proxy_auth REQUIRED
http_access allow ncsa_users
#acl Server2 src 10.100.0.102
#acl client_range src 10.100.0.0/255.255.255.0
#http_access allow Server2 client_range
:wq
```

```
user1@Server1:~/바탕화면$ sudo systemctl restart squid
```

```
user1@Server1:~/바탕화면$ systemctl status squid
```

```
● squid.service - Squid Web Proxy Server
```

```
Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
```

```
Active: active (running) since Tue 2023-08-29 17:18:57 KST; 4s ago
```

```
Docs: man:squid(8)
```

```
Process: 19337 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
```


Server2 나 client_range 이름에 넣고 입력한 비밀번호를 입력한다.

인증 필요 - Mozilla Firefox

moz-proxy://10.100.0.101:3128 프록시가 사용자 이름과 비밀번호를 요청하고 있습니다. 사이트 메시지:
"Squid proxy-caching web server"

사용자 이름

비밀번호

취소 로그인

YouTube

× +

← → ×

https://www.youtube.com

☆

📧 📌 ☰

YouTube

KR

검색

🔍

🎤

⋮

로그인

🏠 홈

📺 Shorts

📁 구독

📺 보관함

🕒 시청 기록

전체

음악

실시간

뉴스

게임

야구

뷰티 팁

관광지

요리

만화 영화

축구

최근에 업로드된 동영상

미국 군인이 외국어를 가장 빨리 배우는 비결

우당탕탕 영어교실 25

0:00 / 23:25

영어독립

이 팩트를 알고 나시면 영어 공부하는 자세가 바뀌게 됩니다.

광고 · 영어독립

Cafe Music

Coffee Shop Ambience

아늑한 커피숍 서적에서 비오는 날 4K 학습/작업을 위한 편안한 재즈 음악 #3

Soul Jazz Music

조회수 363만회 · 7개월 전

SBS NEWS

2천억 원 기금 반납 거부 결국 전액 강제 환수?

SBS

2천억 원 기금 반납 거부...결국 전액 강제 환수? / SBS

SBS 뉴스

조회수 79만회 · 5일 전

SBS CATCH

(싸울 1등)

콜라 좀 사와~

선생님은 일진이라고 안 보줘

트트브 최고에 핑크모은 #B56T-1000

과거 32.2° 현재 15°

옛날이 더 뜨거웠는데 왜 갑자기 호들갑일까?

기후위화: 기후위기

https://www.youtube.com/watch?v=9Tq-G-KSR0A&pp=CkIdXAGQhd6NnJ0Wkw2eUV2VF...z5Fp4N092SEFmdyZsYWJlbD12aWRlbi19lbmRzY3JlZW5FY2xpY2smbXM9W0NMSUNLX01TXSAB

3. 방화벽의 개요

- ❖ 사용자들은 인터넷에 접속하여 다양한 형태의 정보와 서비스를 제공 받고 있다. 그러나 이와 함께 인터넷을 경유한 불법 사용자나 해커들의 침입으로 인한 피해도 늘고 있고, 그 수법 또한 전문적이고 다양해지고 있다.
- ❖ 인터넷으로부터 불법 사용자나 해커의 침입을 막기 위한 대책으로 여러 가지를 사용하지만 일일이 대응 하는 것이 쉬운 일은 아니다.
- ❖ 방화벽은 내부 네트워크와 외부 네트워크의 연결점에서 내부 네트워크 상의 시스템을 보호 할 수 있는 네트워크 구성 요소가 필요하고 이러한 기능을 담당하는 시스템이 바로 방화벽이다.

4. 방화벽 설정 하기

❖ 방화벽 동작 확인하기

```
user1@Server1:~/바탕화면$ dpkg -l | grep ufw
ii  ufw                                0.36.1-4ubuntu0.1
    all                            program for managing a Netfilter firewall
```

```
user1@Server1:~/바탕화면$ sudo ufw status
[sudo] user1 암호:
상태: 비활성
```

```
user1@Server1:~/바탕화면$ sudo ufw enable
방화벽이 활성화 상태이며 시스템이 시작할 때 사용됩니다
user1@Server1:~/바탕화면$ sudo ufw status
상태: 활성
```

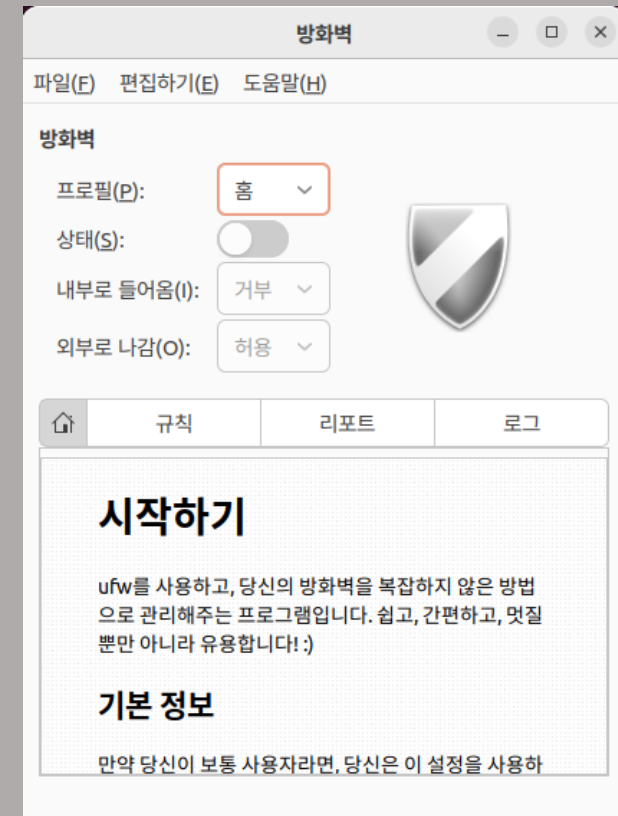
목적	동작	출발
--	--	--
53	ALLOW	Anywhere
53 (v6)	ALLOW	Anywhere (v6)

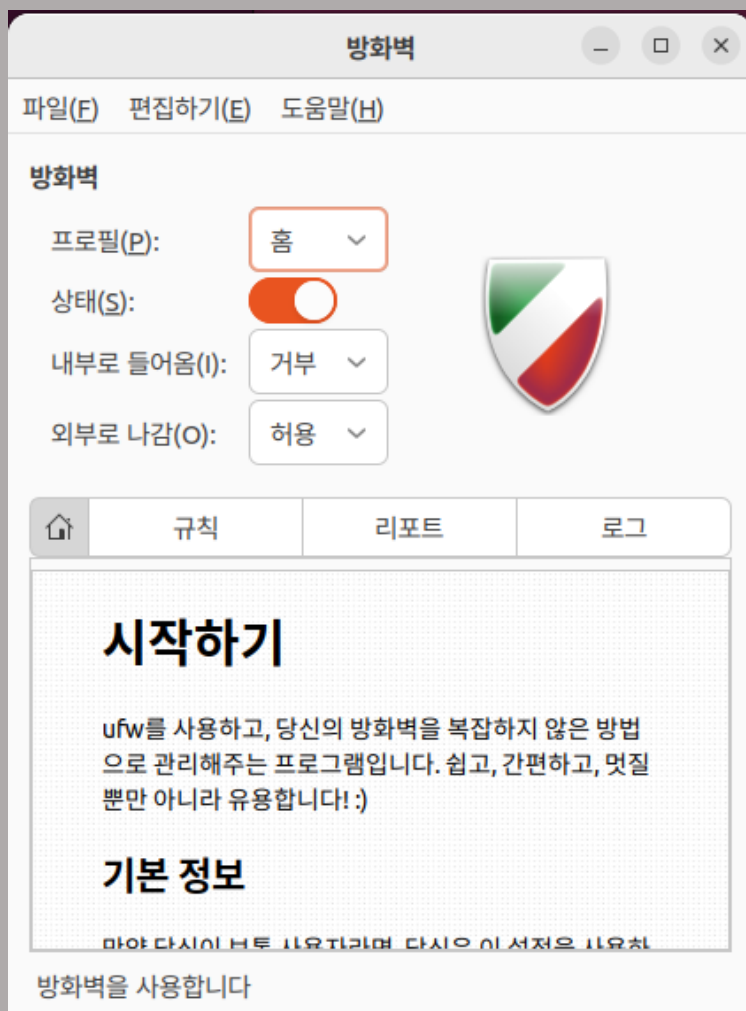
```
user1@Server1:~/바탕화면$ sudo ufw disable
방화벽이 비활성 되었으며 시스템이 시작할 때 사용되지 않습니다
```


❖ GUI 도구로 방화벽 설정하기

```
user1@Server1:~/바탕화면$ sudo apt-get install gufw
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다... 완료
상태 정보를 읽는 중입니다... 완료
다음 새 패키지를 설치할 것입니다:
  gufw
0개 업그레이드, 1개 새로 설치, 0개 제거 및 27개 업그레이드 안 함.
```

```
user1@Server1:~/바탕화면$ sudo gufw
```





프로필 : 현재 설정하는 내용을 적용할 환경을 설정한다.

상태 : 방화벽 전체를 끄거나 켤 수 있다.

내부로 들어옴 : 시스템 내부로 들어오는 트래픽 설정이다.

외부로 나감 : 시스템 외부로 보내는 트래픽 설정이다.

(내부로 들어옴 거부, 외부로 나감 허용은 기본값이다)

규칙 : 규칙을 선택하면 현재 적용 중인 규칙을 보여준다.

리포트 : 현재 열려 있는 포트를 보고 한다.

로그 : 방화벽과 관련된 로그 기록을 보여 준다.

❖ 방화벽 관리 명령

ufw	
기능	방화벽을 설정한다.
형식	ufw [서브 명령]
옵션	<p>enable : 방화벽을 활성화 한다.</p> <p>disable : 방화벽을 비활성화 한다.</p> <p>default [allow deny reject] [incoming outgoing] : 방화벽의 기본 동작을 설정한다.</p> <p>status [verbose] : 방화벽의 상태를 출력한다.</p> <p>allow [서비스 포트/프로토콜] : 지정한 서비스나 포트를 허용한다.</p> <p>deny [서비스 포트/프로토콜] : 지정한 서비스나 포트를 거부한다.</p> <p>delete [명령] : 명령으로 설정한 규칙을 삭제한다.</p>

❖ 방화벽의 상태 보기

```
user1@Server1:~/바탕화면$ sudo ufw status  
상태: 활성
```

❖ 규칙 추가하기

```
user1@Server1:~/바탕화면$ sudo ufw allow http
```

규칙이 추가되었습니다

규칙이 추가되었습니다 (v6)

```
user1@Server1:~/바탕화면$ sudo ufw status
```

상태: 활성

목적	동작	출발
--	--	--
80/tcp	ALLOW	Anywhere
80/tcp (v6)	ALLOW	Anywhere (v6)

❖ 서비스 거부하기

```
user1@Server1:~/바탕화면$ sudo ufw deny telnet
```

규칙이 추가되었습니다

규칙이 추가되었습니다 (v6)

```
user1@Server1:~/바탕화면$ sudo ufw status
```

상태: 활성

목적	동작	출발
--	--	--
80/tcp	ALLOW	Anywhere
23/tcp	DENY	Anywhere
80/tcp (v6)	ALLOW	Anywhere (v6)
23/tcp (v6)	DENY	Anywhere (v6)

❖ 규칙 삭제하기

```
user1@Server1:~/바탕화면$ sudo ufw delete deny telnet
규칙이 삭제되었습니다
규칙이 삭제되었습니다 (v6)
```

❖ 포트 추가하기

```
user1@Server1:~/바탕화면$ sudo ufw allow 5000/tcp
규칙이 추가되었습니다
규칙이 추가되었습니다 (v6)
```

```
user1@Server1:~/바탕화면$ sudo ufw status
상태: 활성
```

목적	동작	출발
--	--	--
80/tcp	ALLOW	Anywhere
5000/tcp	ALLOW	Anywhere
80/tcp (v6)	ALLOW	Anywhere (v6)
5000/tcp (v6)	ALLOW	Anywhere (v6)

❖ 특정 IP 주소의 접속 설정하기

```
user1@Server1:~/바탕화면$ sudo ufw allow from 10.100.0.102 to any port ftp
규칙이 추가되었습니다
```

```
user1@Server1:~/바탕화면$ sudo ufw status
```

상태: 활성

목적	동작	출발
--	--	--
80/tcp	ALLOW	Anywhere
5000/tcp	ALLOW	Anywhere
21/tcp	ALLOW	10.100.0.102
80/tcp (v6)	ALLOW	Anywhere (v6)
5000/tcp (v6)	ALLOW	Anywhere (v6)

Quiz

❖ Server2 에 아래와 같이 실습 해 본다.

- 프록시 서버를 설치한다.
- Server1 에서 프록시를 이용해서 외부 사이트 접속 및 프록시 서버 사용이 잘 되는지 확인 해 본다.
- 프록시가 잘 되는 상황에서 프록시 포트를 방화벽으로 막아 보고 프록시 서버에 접근이 잘 되는지 확인 해 본다.

A photograph of a server room with rows of server racks on both sides of a central aisle. The racks have glass doors and internal components are visible, with many small blue lights glowing. The ceiling has several long, rectangular light fixtures. The overall atmosphere is dimly lit, emphasizing the blue light from the servers.

수고하셨습니다.