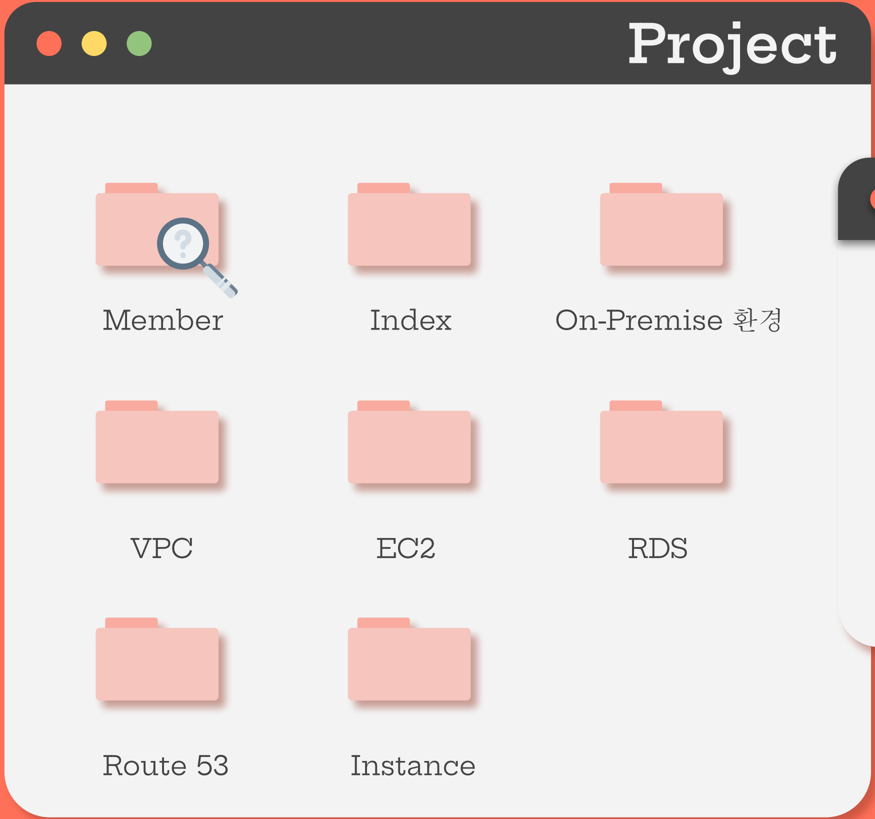
AWS
Business Network Migration Project

Start now!



Project

Member

Index

On-Premise 환경

VPC

EC2

RDS

Route 53

Instance

Member

김성주

서진희

Index

On-Premise 환경

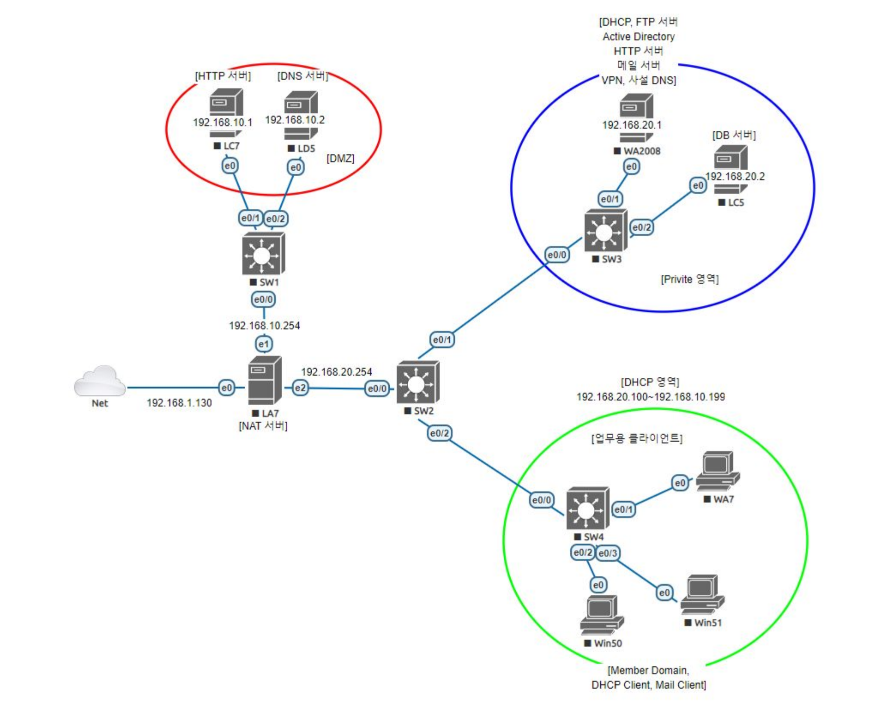
기존 사내 System Environmet

AWS Cloud Migration

AWS 환경으로의 이전

- 보안성을 위해 OS 업그레이드
- 최신버전의 프로그램

On-Premise 환경

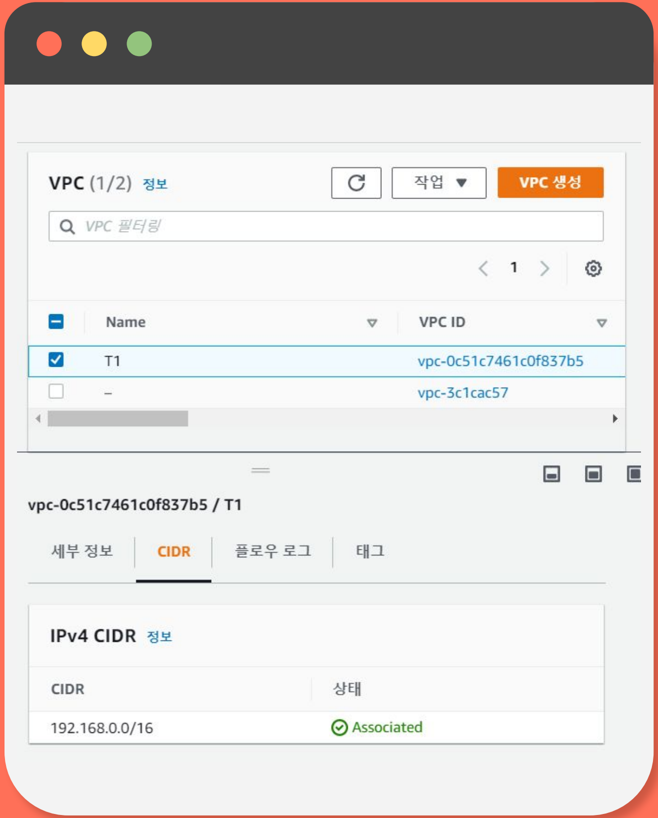


1 NAT 서버

2 DMZ 영역
- HTTP 서버(CentOS 7)
- DNS 서버(CentOS 5)
  - projectt1.net

3. Pirvate 영역
- DB 서버(MySQL 5.7)
- Windows Server 2008 R2
  - 사내 DNS
  - Actvie Directory
  - DHCP
  - FTP, HTTP
  - VPN
  - Mail Server

VPC



VPC (1/2) 정보

☐	Name	VPC ID
☑	T1	vpc-0c51c7461c0f837b5
□	–	vpc-3c1cac57

vpc-0c51c7461c0f837b5 / T1

세부 정보 | CIDR | 플로우 로그 | 태그

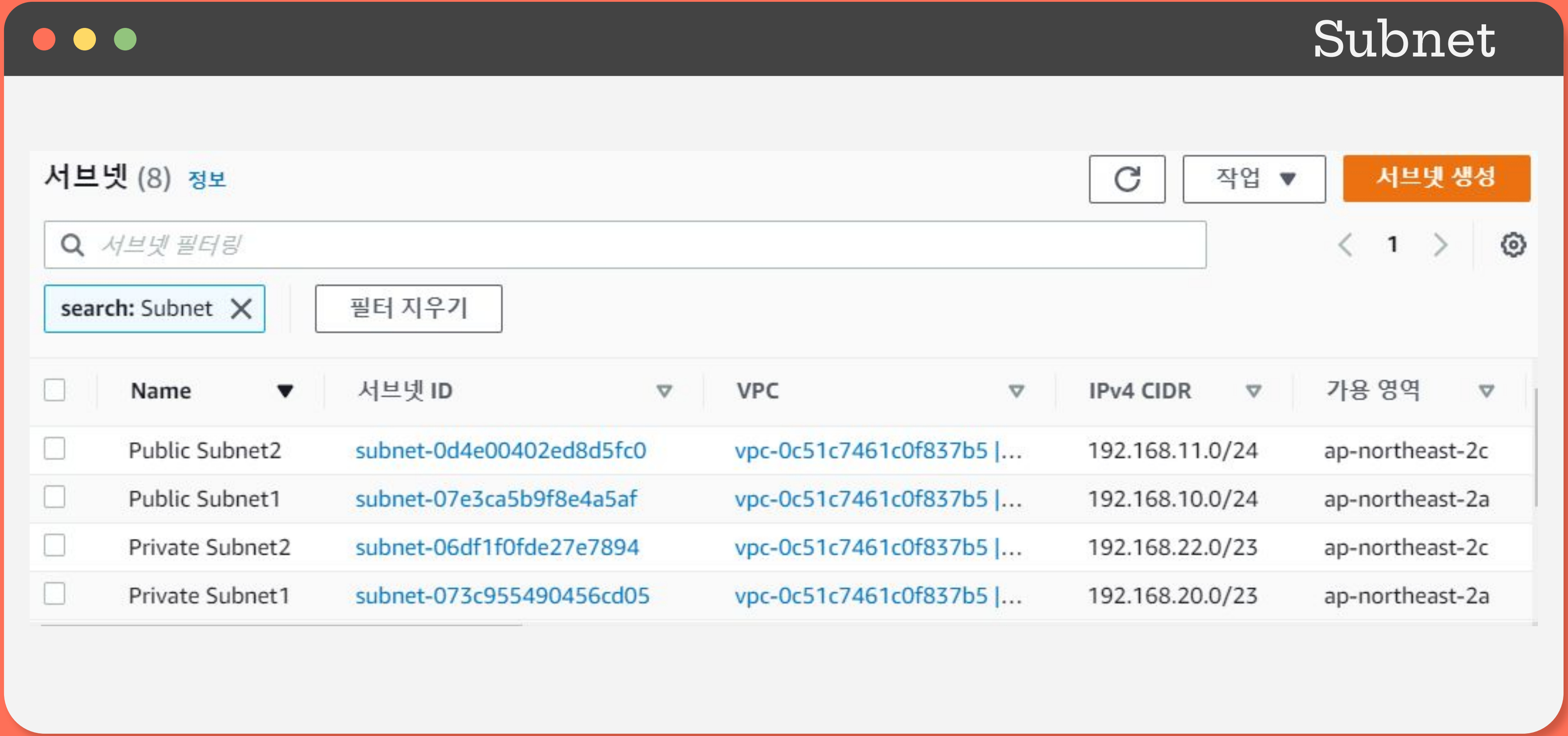
IPv4 CIDR 정보

CIDR	상태
192.168.0.0/16	✓ Associated

VPC 환경

Name : T1

CIDR : 192.168.0.0/16



Subnet

서브넷 (8) 정보

search: Subnet ✕

□	Name	서브넷 ID	VPC	IPv4 CIDR	가용 영역
□	Public Subnet2	subnet-0d4e00402ed8d5fc0	vpc-0c51c7461c0f837b5 |...	192.168.11.0/24	ap-northeast-2c
□	Public Subnet1	subnet-07e3ca5b9f8e4a5af	vpc-0c51c7461c0f837b5 |...	192.168.10.0/24	ap-northeast-2a
□	Private Subnet2	subnet-06df1f0fde27e7894	vpc-0c51c7461c0f837b5 |...	192.168.22.0/23	ap-northeast-2c
□	Private Subnet1	subnet-073c955490456cd05	vpc-0c51c7461c0f837b5 |...	192.168.20.0/23	ap-northeast-2a

Public Subnet1

VPC	: T1
CIDR	: 192.168.10.0/24
Availability Zone	: ap-northeast-2a

Public Subnet2

VPC	: T1
CIDR	: 192.168.11.0/24
Availability Zone	: ap-northeast-2c

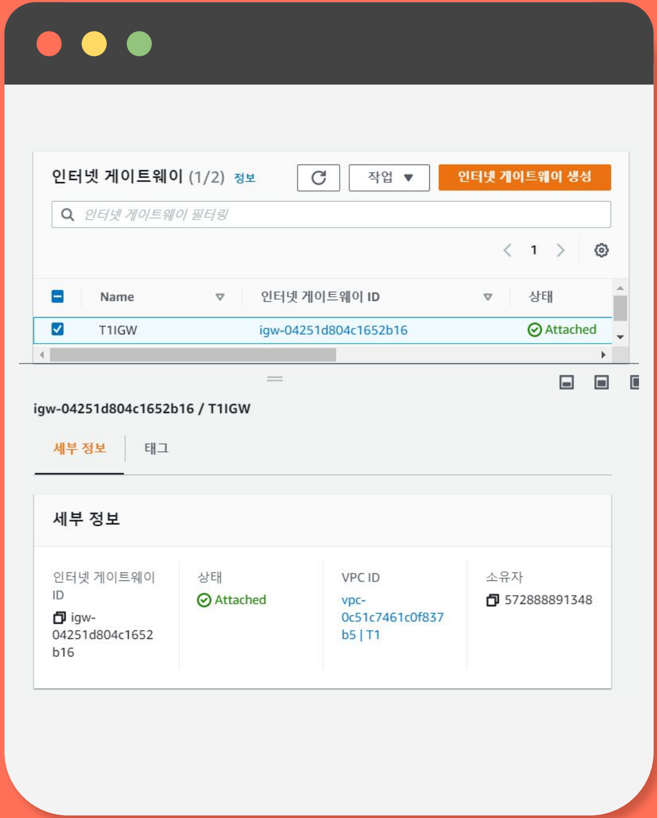
Private Subnet1

VPC	: T1
CIDR	: 192.168.20.0/23
Availability Zone	: ap-northeast-2a

Private Subnet2

VPC	: T1
CIDR	: 192.168.22.0/23
Availability Zone	: ap-northeast-2c

Internet Gateway



인터넷 게이트웨이 (1/2) 정보

☐	Name	인터넷 게이트웨이 ID	상태
☑	T1IGW	igw-04251d804c1652b16	✓ Attached

igw-04251d804c1652b16 / T1IGW

세부 정보

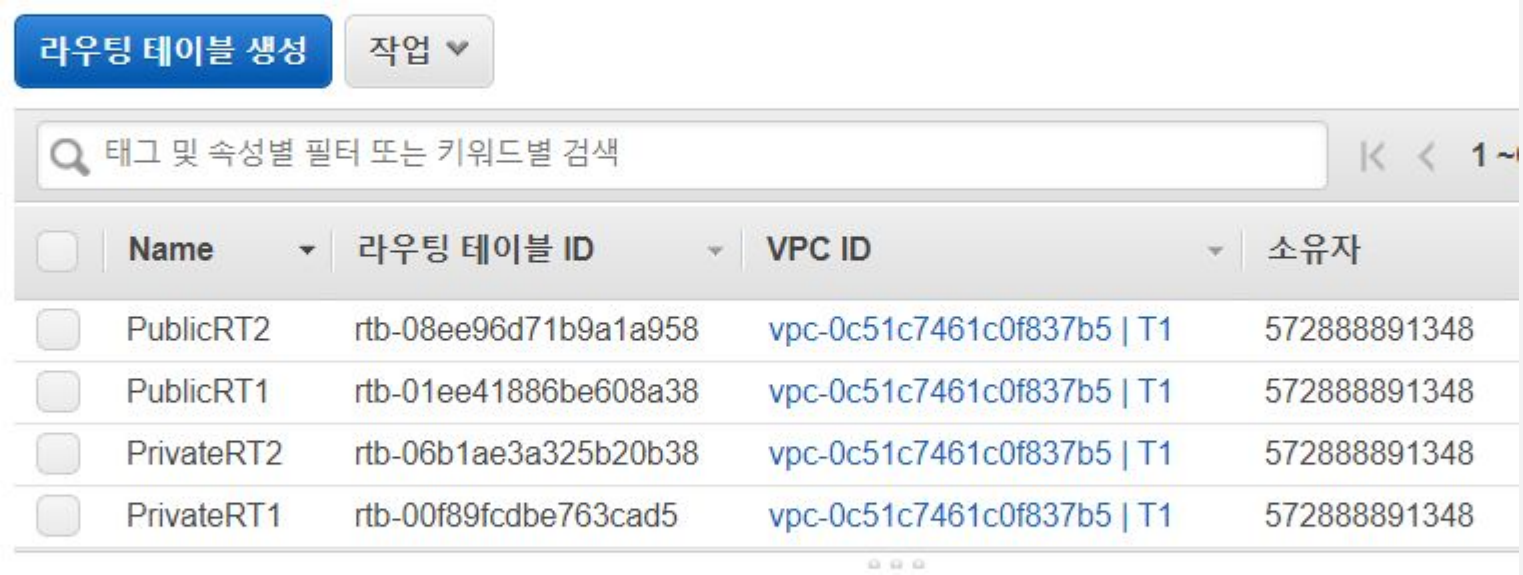
인터넷 게이트웨이 ID	상태	VPC ID	소유자
igw-04251d804c1652b16	✓ Attached	vpc-0c51c7461c0f837b5 | T1	572888891348

Internet Gateway

Name : T1IGW

Attach VPC : T1

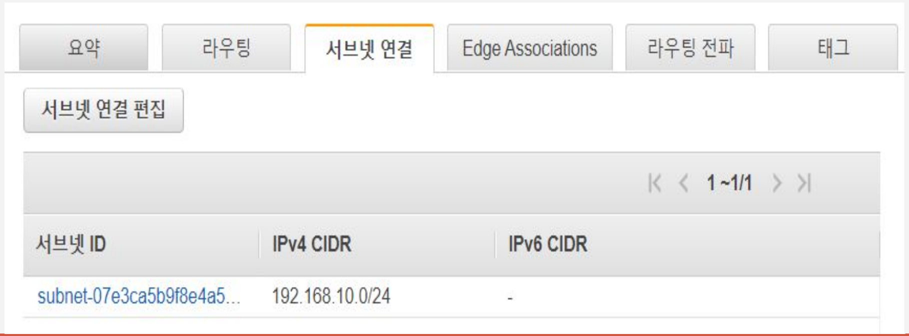
Route Table



□	Name	라우팅 테이블 ID	VPC ID	소유자
□	PublicRT2	rtb-08ee96d71b9a1a958	vpc-0c51c7461c0f837b5 | T1	572888891348
□	PublicRT1	rtb-01ee41886be608a38	vpc-0c51c7461c0f837b5 | T1	572888891348
□	PrivateRT2	rtb-06b1ae3a325b20b38	vpc-0c51c7461c0f837b5 | T1	572888891348
□	PrivateRT1	rtb-00f89fcdbe763cad5	vpc-0c51c7461c0f837b5 | T1	572888891348

Route Table

PublicRT1

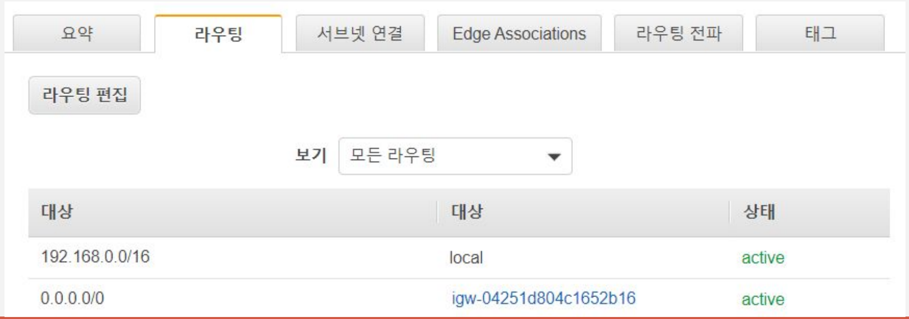


서브넷 ID	IPv4 CIDR	IPv6 CIDR
subnet-07e3ca5b9f8e4a5...	192.168.10.0/24	-

연결된 Subnet

→ Public Subnet 1

PublicRT1



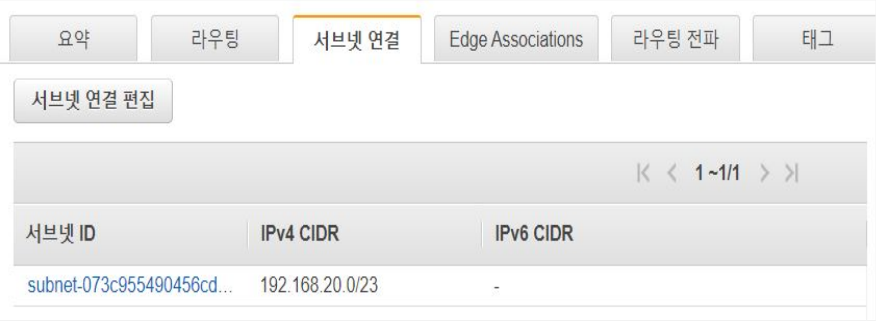
보기: 모든 라우팅

대상	대상	상태
192.168.0.0/16	local	active
0.0.0.0/0	igw-04251d804c1652b16	active

Internet Gateway (T1IGW)와 연결

Route Table

PrivateRT1

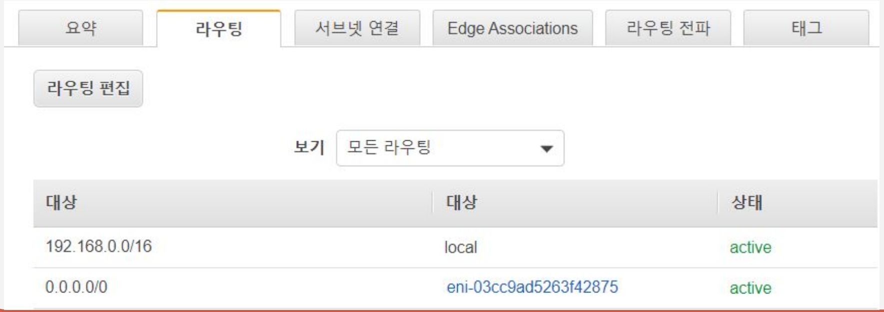


서브넷 ID	IPv4 CIDR	IPv6 CIDR
subnet-073c955490456cd...	192.168.20.0/23	-

연결된 Subnet

→ Private Subnet 1

PrivateRT1

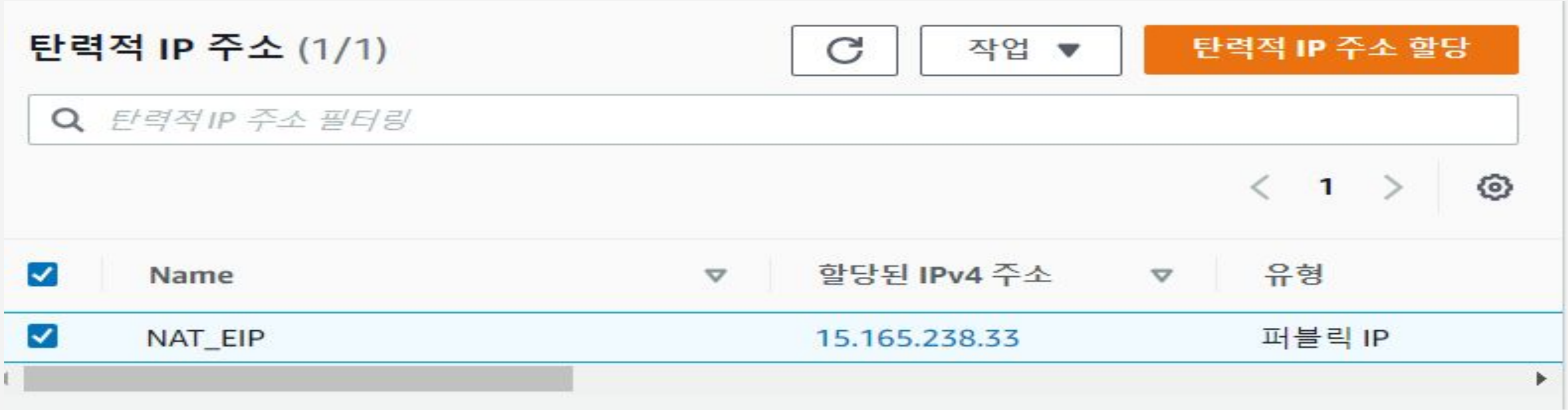


보기 모든 라우팅

대상	대상	상태
192.168.0.0/16	local	active
0.0.0.0/0	eni-03cc9ad5263f42875	active

Nat Instance와 연결

Elastic IP



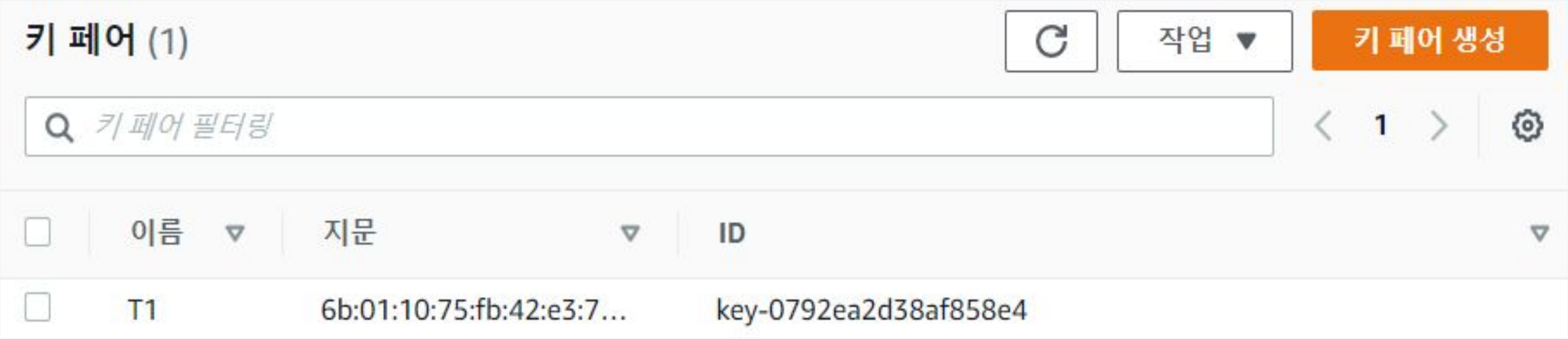
☑	Name	할당된 IPv4 주소	유형
☑	NAT_EIP	15.165.238.33	퍼블릭 IP

Elastic IP

- 이름 : NAT_EIP
- 연결된 인스턴스 : NAT Instance

EC2

Key Pair 생성



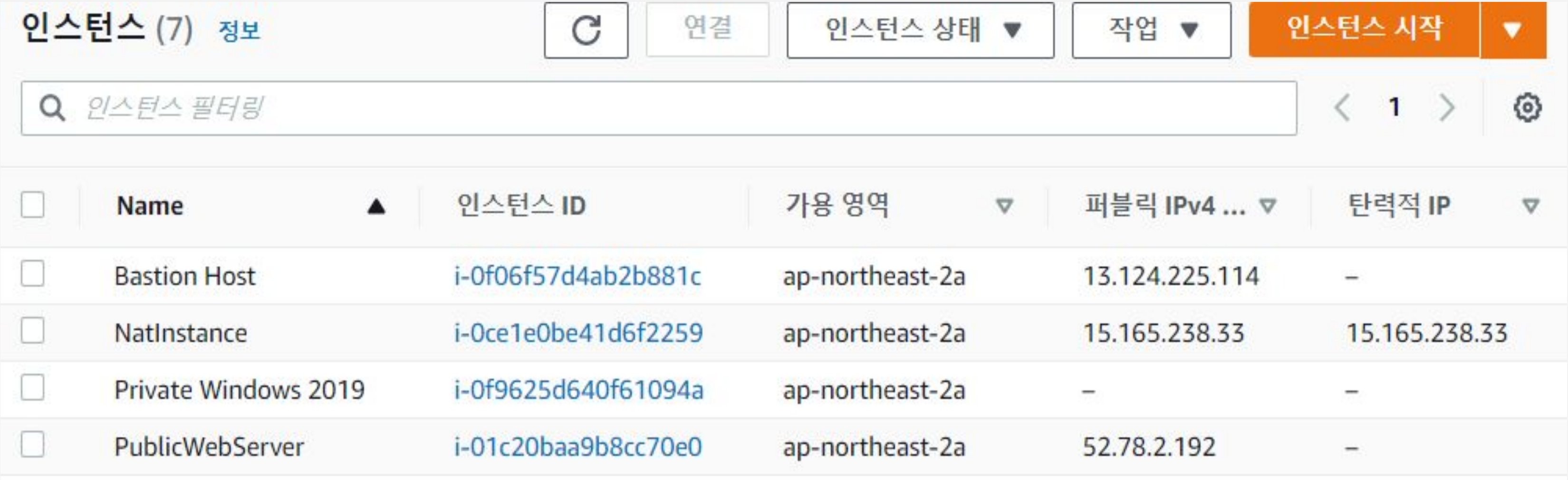
키 페어 (1)

□	이름	지문	ID
□	T1	6b:01:10:75:fb:42:e3:7...	key-0792ea2d38af858e4

Key Pair 생성

Name : T1

Instance



□	Name ▲	인스턴스 ID	가용 영역 ▽	퍼블릭 IPv4 ... ▽	탄력적 IP ▽
□	Bastion Host	i-0f06f57d4ab2b881c	ap-northeast-2a	13.124.225.114	–
□	NatInstance	i-0ce1e0be41d6f2259	ap-northeast-2a	15.165.238.33	15.165.238.33
□	Private Windows 2019	i-0f9625d640f61094a	ap-northeast-2a	–	–
□	PublicWebServer	i-01c20baa9b8cc70e0	ap-northeast-2a	52.78.2.192	–

Bastion Host

- 서버 관리용 인스턴스

Nat Instance

- Private 영역 내 서비스 접근 허용
- 인스턴스 보안성 향상

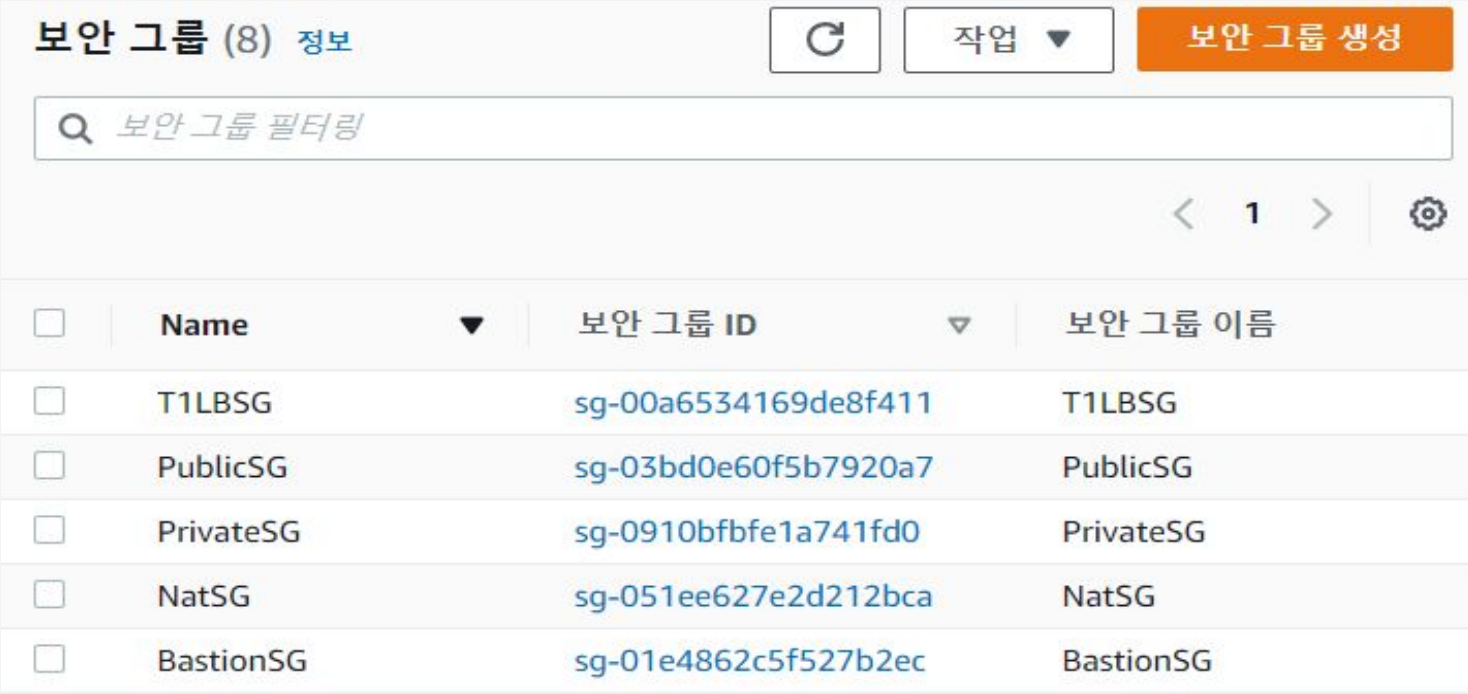
PublicWebServer

- Public Subnet에 위치
- 실행 서비스
  → HTTP

Private Windows 2019

- Pirvate Subnet 위치
- 실행 서비스
  → HTTP, FTP, Mail, VPN,
  Active Directory

Security Group



보안 그룹 (8) 정보

□	Name ▼	보안 그룹 ID ▽	보안 그룹 이름
□	T1LBSG	sg-00a6534169de8f411	T1LBSG
□	PublicSG	sg-03bd0e60f5b7920a7	PublicSG
□	PrivateSG	sg-0910bfbfe1a741fd0	PrivateSG
□	NatSG	sg-051ee627e2d212bca	NatSG
□	BastionSG	sg-01e4862c5f527b2ec	BastionSG

Security Group

Name	기능	Name	기능
BastionSG	Bastion Host 보안그룹	PublicSG	PublicWebServer 보안그룹
NatSG	Nat Instance 보안그룹	PrivateSG	Private Windows 2019 보안그룹
T1LBSG	ELB 보안그룹		

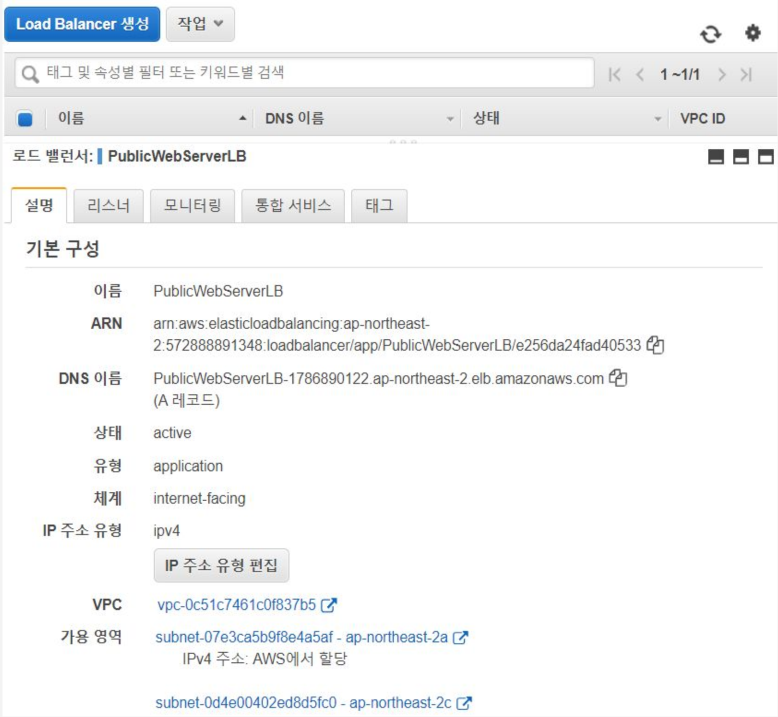
NatSG

기능	Port	기능	Port	기능	Port
FTP	TCP 20,21	DNS	TCP/UDP 53	NTP	TCP 123
SMTP	TCP 25	HTTP	TCP 80	RPC	TCP/UDP 135
Wins Replication	TCP/UDP 42	Keyberos	TCP/UDP 88	netbios nameserver	TCP/UDP 137
GRE	TCP 47	POP3	TCP 110	netbios datagram service	UDP 138

NatSG

기능	Port	기능	Port	기능	Port
netbios session service	TCP 139	IPSec lSKMP	UDP 500	PPTP	TCP 1723
LDAP	TCP/UDP 389	LDAP OVER SSL	TCP 636	Global Catalog LDAP	TCP/UDP 3268
SMB Over ip	TCP/UDP 445	Wins resolution	TCP/UDP 1512	Global Catalog LDAP Over SSL	TCP/UDP 3269
Keyberos 암호 변경	TCP/UDP 464	L2TP	TCP 1701	IPSec	UDP 4500

ELB



로드 밸런서: PublicWebServerLB

기본 구성

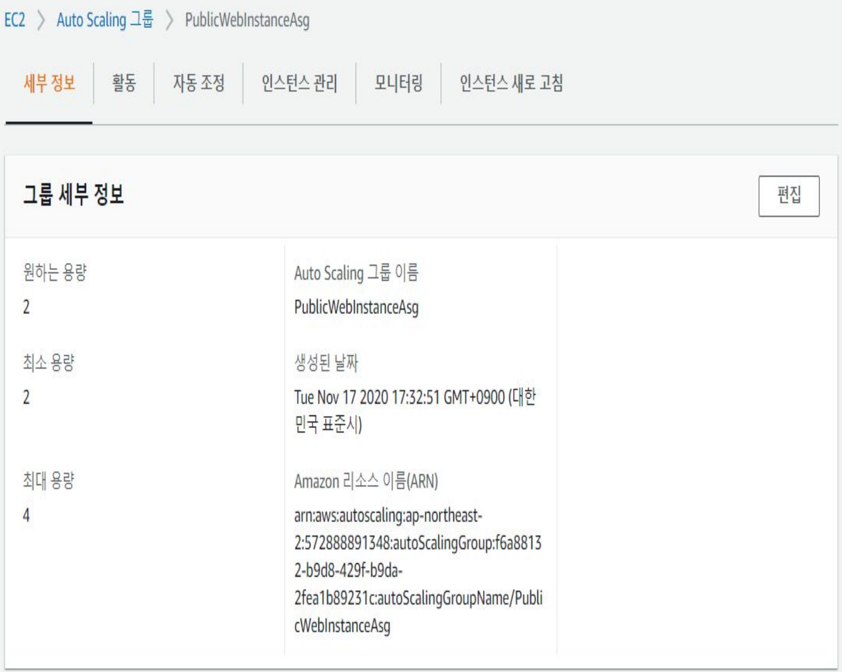
이름	PublicWebServerLB
ARN	arn:aws:elasticloadbalancing:ap-northeast-2:572888891348:loadbalancer/app/PublicWebServerLB/e256da24fad40533
DNS 이름	PublicWebServerLB-1786890122.ap-northeast-2.elb.amazonaws.com (A 레코드)
상태	active
유형	application
체계	internet-facing
IP 주소 유형	ipv4
VPC	vpc-0c51c7461c0f837b5
가용 영역	subnet-07e3ca5b9f8e4a5af - ap-northeast-2a IPv4 주소: AWS에서 할당 subnet-0d4e00402ed8d5fc0 - ap-northeast-2c

Name
→ PublicWebServerLB

Target Instance
→ PublicWebServer

Availability Zone
→ ap-northeast-2a
→ ap-northeast-2c

Auto Scaling



EC2 〉 Auto Scaling 그룹 〉 PublicWebInstanceAsg

그룹 세부 정보

원하는 용량
2

최소 용량
2

최대 용량
4

Auto Scaling 그룹 이름
PublicWebInstanceAsg

생성된 날짜
Tue Nov 17 2020 17:32:51 GMT+0900 (대한민국 표준시)

Amazon 리소스 이름(ARN)
arn:aws:autoscaling:ap-northeast-2:572888891348:autoScalingGroup:f6a88132-b9d8-429f-b9da-2fea1b89231c:autoScalingGroupName/PublicWebInstanceAsg

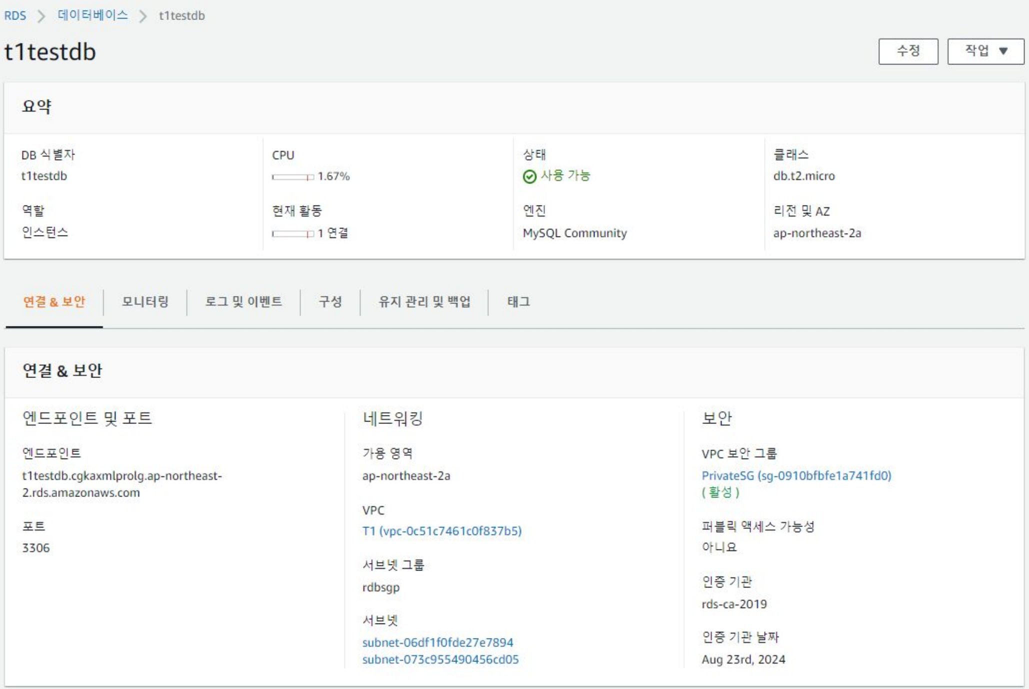
Name
→ PublicWebServerAsg

Target Instance
→ PublicWebServer

Size
→ Default : 2
→ Min : 2
→ Max : 4

RDS

RDS



RDS > 데이터베이스 > t1testdb

t1testdb

요약

DB 식별자 t1testdb	CPU 1.67%	상태 ✓ 사용 가능	클래스 db.t2.micro
역할 인스턴스	현재 활동 1 연결	엔진 MySQL Community	리전 및 AZ ap-northeast-2a

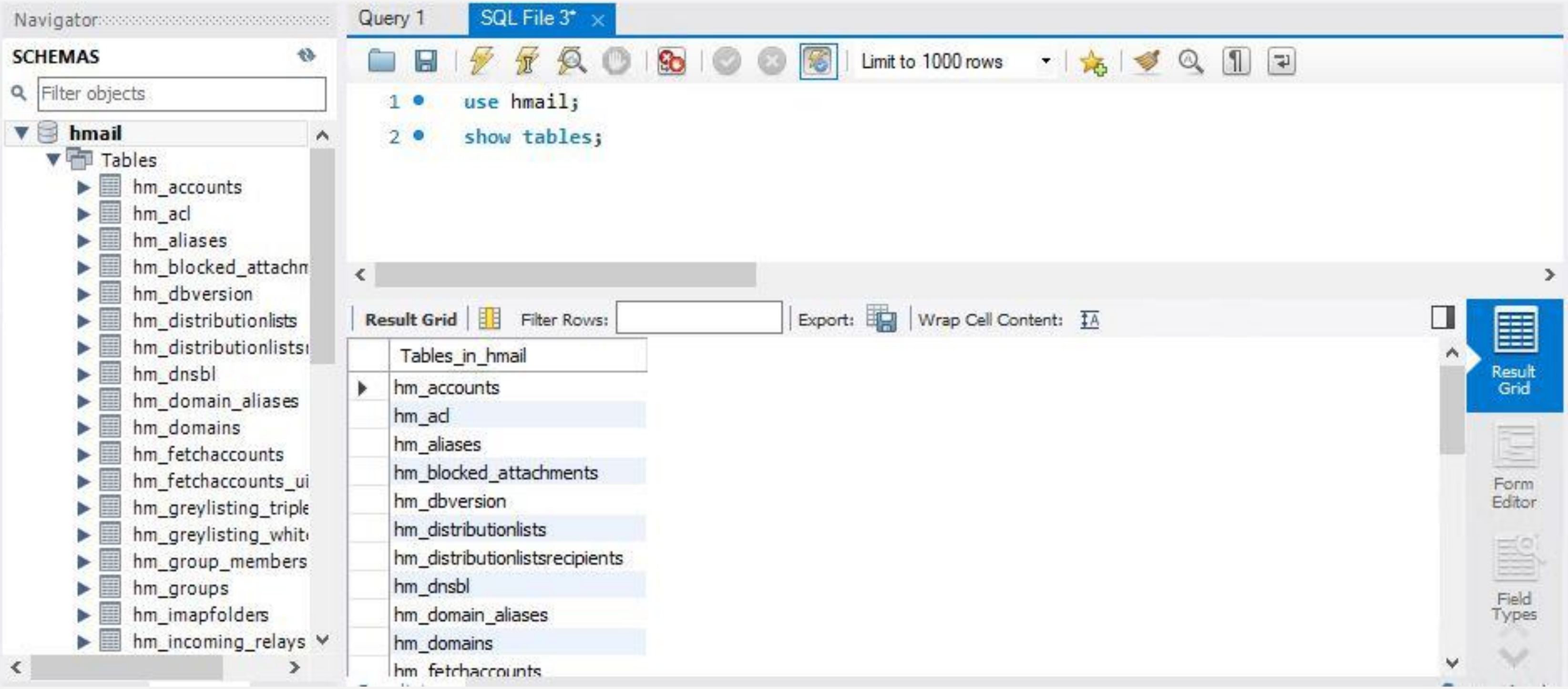
연결 & 보안

엔드포인트 및 포트	네트워킹	보안
엔드포인트 t1testdb.cgkaxmlprolg.ap-northeast-2.rds.amazonaws.com	가용 영역 ap-northeast-2a	VPC 보안 그룹 PrivateSG (sg-0910bfbfe1a741fd0) (활성)
포트 3306	VPC T1 (vpc-0c51c7461c0f837b5)	퍼블릭 액세스 가능성 아니요
	서브넷 그룹 rdbsgp	인증 기관 rds-ca-2019
	서브넷 subnet-06df1f0fde27e7894 subnet-073c955490456cd05	인증 기관 날짜 Aug 23rd, 2024

Name
→ t1testdb

DB Type
→ MySQL 5.7

RDS Access



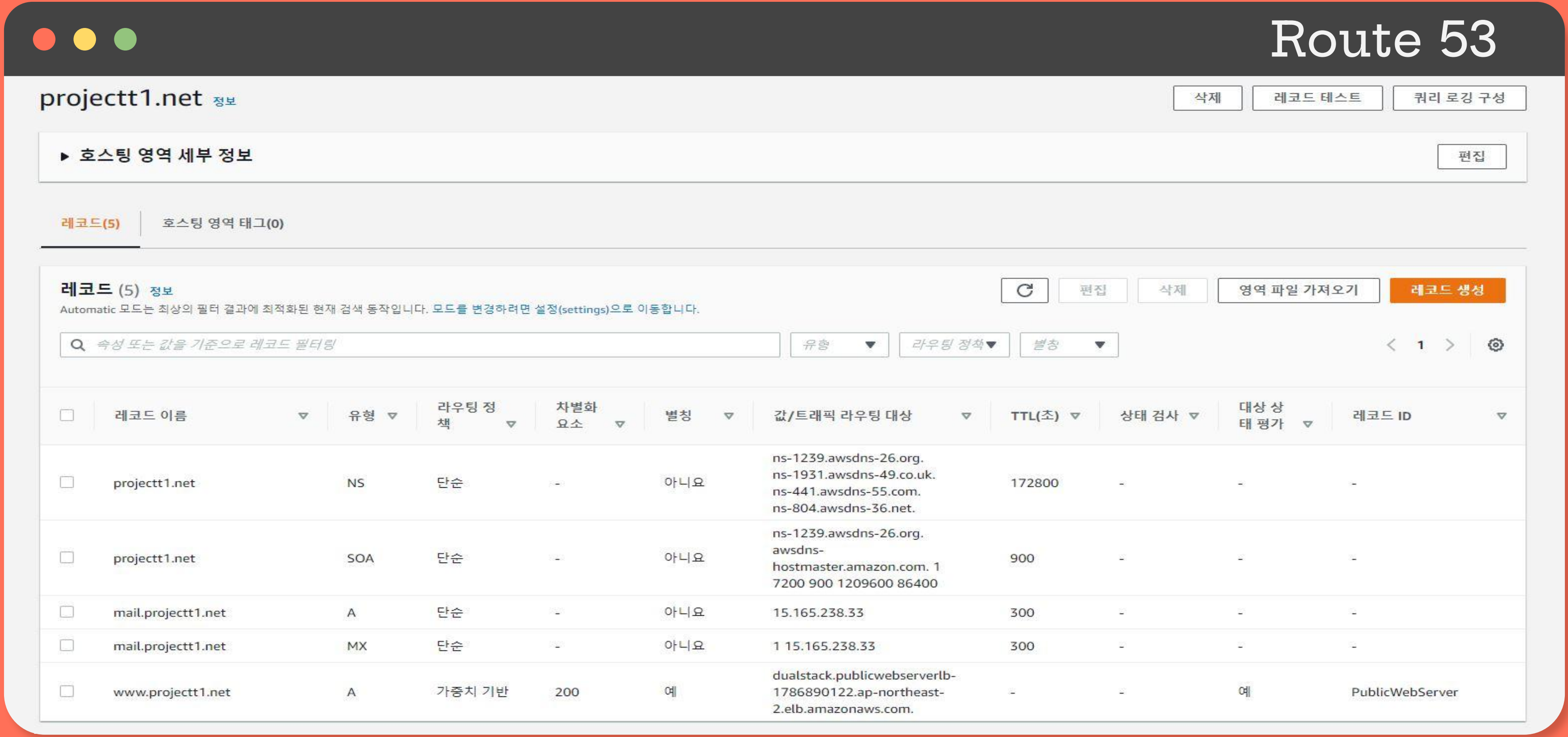
- hmail
  - Tables
    - hm_accounts
    - hm_acl
    - hm_aliases
    - hm_blocked_attachm
    - hm_dbversion
    - hm_distributionlists
    - hm_distributionlistsı
    - hm_dnsbl
    - hm_domain_aliases
    - hm_domains
    - hm_fetchaccounts
    - hm_fetchaccounts_ui
    - hm_greylisting_triple
    - hm_greylisting_whit
    - hm_group_members
    - hm_groups
    - hm_imapfolders
    - hm_incoming_relays

```
use hmail;
show tables;
```

Tables_in_hmail
hm_accounts
hm_acl
hm_aliases
hm_blocked_attachments
hm_dbversion
hm_distributionlists
hm_distributionlistsrecipients
hm_dnsbl
hm_domain_aliases
hm_domains
hm_fetchaccounts

Route 53

Route 53



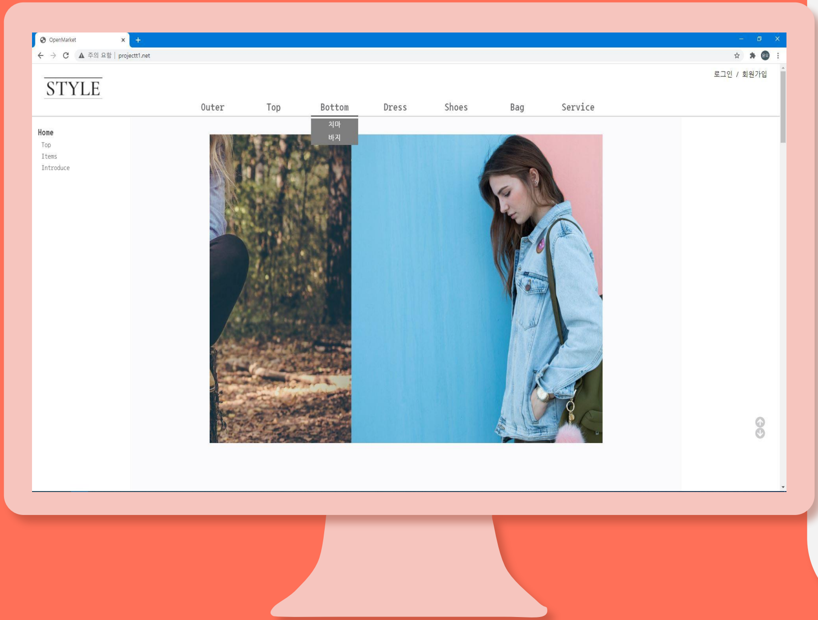
projectt1.net 정보

▸ 호스팅 영역 세부 정보

레코드 (5) 정보

Automatic 모드는 최상의 필터 결과에 최적화된 현재 검색 동작입니다. 모드를 변경하려면 설정(settings)으로 이동합니다.

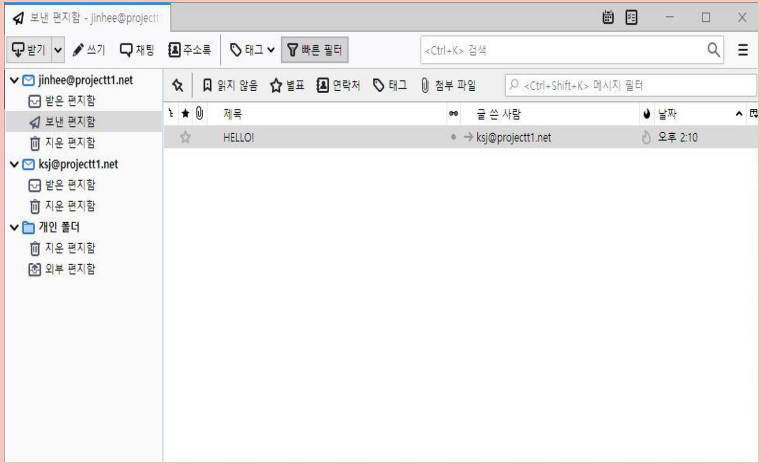
□	레코드 이름	유형	라우팅 정책	차별화 요소	별칭	값/트래픽 라우팅 대상	TTL(초)	상태 검사	대상 상태 평가	레코드 ID
□	projectt1.net	NS	단순	-	아니요	ns-1239.awsdns-26.org. ns-1931.awsdns-49.co.uk. ns-441.awsdns-55.com. ns-804.awsdns-36.net.	172800	-	-	-
□	projectt1.net	SOA	단순	-	아니요	ns-1239.awsdns-26.org. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400	900	-	-	-
□	mail.projectt1.net	A	단순	-	아니요	15.165.238.33	300	-	-	-
□	mail.projectt1.net	MX	단순	-	아니요	1 15.165.238.33	300	-	-	-
□	www.projectt1.net	A	가중치 기반	200	예	dualstack.publicwebserverlb-1786890122.ap-northeast-2.elb.amazonaws.com.	-	-	예	PublicWebServer



Route 53

www.projectt1.net

- PublicWebServer Instance Web Service
- 인터넷 상에서 서비스



제목	글 쓴 사람	날짜
HELLO!	ksj@projectt1.net	오후 2:10

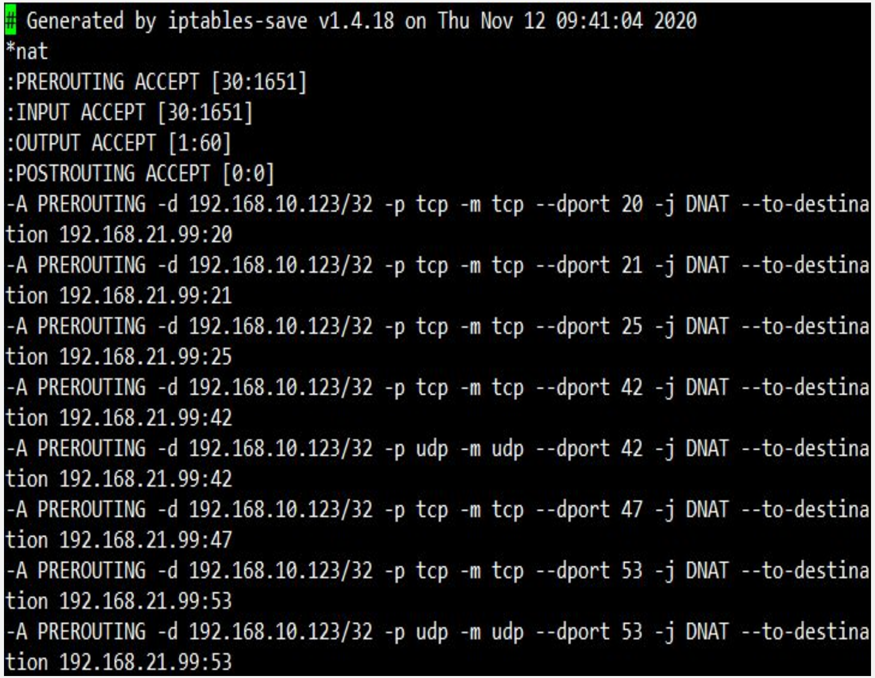
Route 53

[계정명]@projectt1.net

- Private Windows 2019 Mail Service
- 회사 메일 서버

Instance

Nat Instance

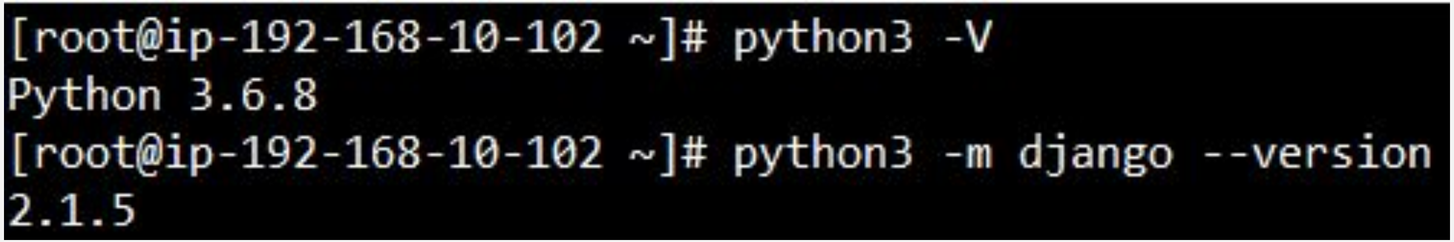


```
# Generated by iptables-save v1.4.18 on Thu Nov 12 09:41:04 2020
*nat
:PREROUTING ACCEPT [30:1651]
:INPUT ACCEPT [30:1651]
:OUTPUT ACCEPT [1:60]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -d 192.168.10.123/32 -p tcp -m tcp --dport 20 -j DNAT --to-destina
tion 192.168.21.99:20
-A PREROUTING -d 192.168.10.123/32 -p tcp -m tcp --dport 21 -j DNAT --to-destina
tion 192.168.21.99:21
-A PREROUTING -d 192.168.10.123/32 -p tcp -m tcp --dport 25 -j DNAT --to-destina
tion 192.168.21.99:25
-A PREROUTING -d 192.168.10.123/32 -p tcp -m tcp --dport 42 -j DNAT --to-destina
tion 192.168.21.99:42
-A PREROUTING -d 192.168.10.123/32 -p udp -m udp --dport 42 -j DNAT --to-destina
tion 192.168.21.99:42
-A PREROUTING -d 192.168.10.123/32 -p tcp -m tcp --dport 47 -j DNAT --to-destina
tion 192.168.21.99:47
-A PREROUTING -d 192.168.10.123/32 -p tcp -m tcp --dport 53 -j DNAT --to-destina
tion 192.168.21.99:53
-A PREROUTING -d 192.168.10.123/32 -p udp -m udp --dport 53 -j DNAT --to-destina
tion 192.168.21.99:53
```

Iptables 기능 이용

1. NAT_EIP 주소 입력
2. Nat Instance에서 Private Windows 2019의 IP주소 변경
3. Pirvate Windows 2019에 실행중인 서비스 접근

PublicWebServer



```
[root@ip-192-168-10-102 ~]# python3 -V
Python 3.6.8
[root@ip-192-168-10-102 ~]# python3 -m django --version
2.1.5
```

PublicWebServer

환경
OS : CentOS 7
Python : 3.6.8
Django : 2.1.5

Private Windows 2019

Private Windows 2019

1 Active Directory

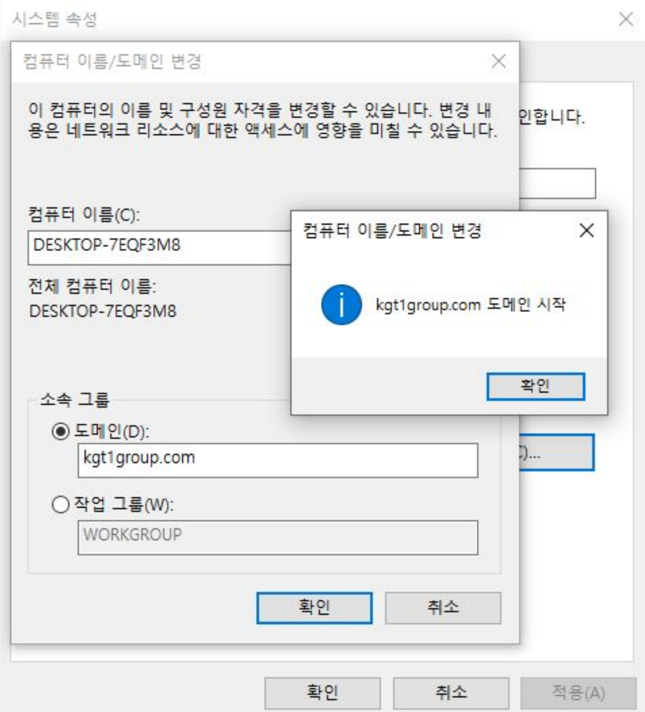
2 Mail Server

3 VPN(L2TP)

4 FTP

5 HTTP

Active Directory



시스템 속성

컴퓨터 이름/도메인 변경

이 컴퓨터의 이름 및 구성원 자격을 변경할 수 있습니다. 변경 내용은 네트워크 리소스에 대한 액세스에 영향을 미칠 수 있습니다.

인합니다.

컴퓨터 이름(C):
DESKTOP-7EQF3M8

전체 컴퓨터 이름:
DESKTOP-7EQF3M8

소속 그룹

● 도메인(D):
kgt1group.com

○ 작업 그룹(W):
WORKGROUP

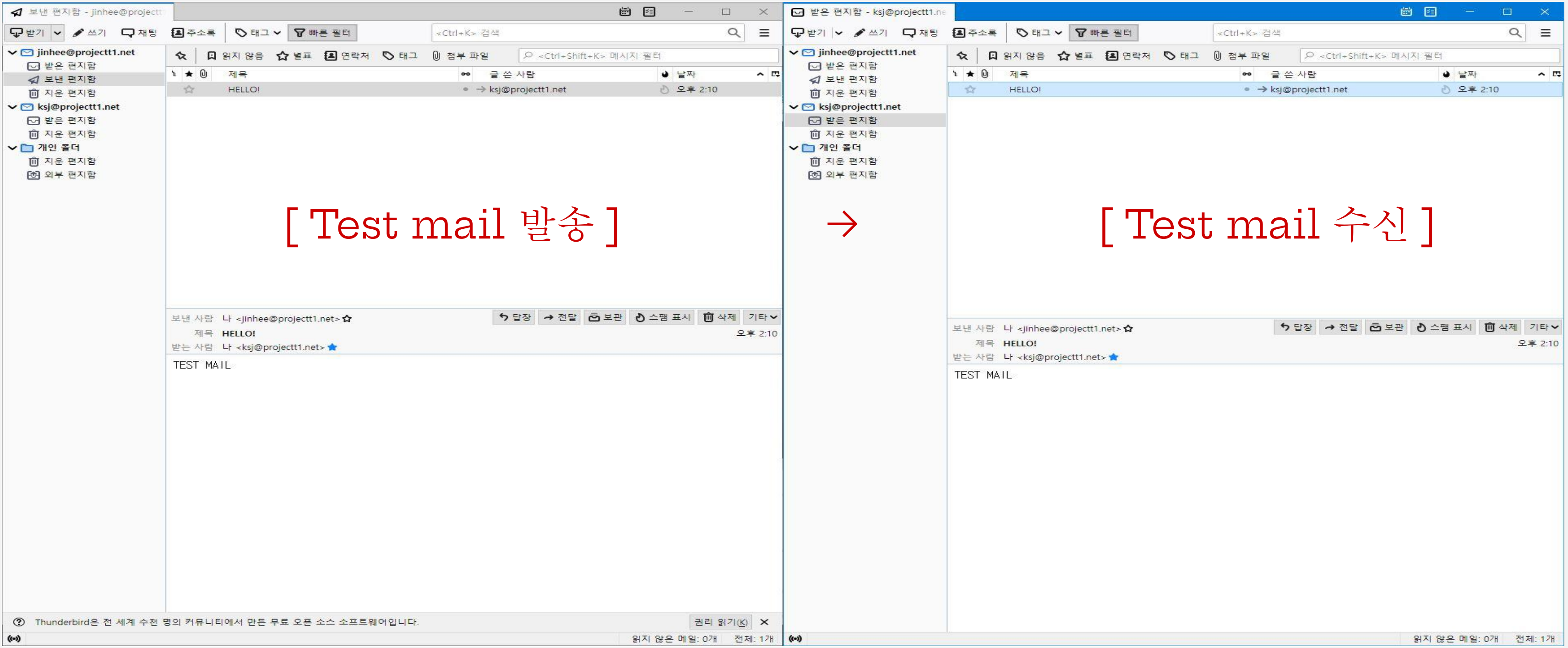
컴퓨터 이름/도메인 변경

kgt1group.com 도메인 시작

Active Directory

- Domain : kgt1group.com
- Client에서 Domain 가입

Mail Server



제목	글 쓴 사람	날짜
HELLO!	→ ksj@projectt1.net	오후 2:10

보낸 사람 나 <jinhee@projectt1.net>
제목 HELLO!
받는 사람 나 <ksj@projectt1.net>
오후 2:10

TEST MAIL

Thunderbird은 전 세계 수천 명의 커뮤니티에서 만든 무료 오픈 소스 소프트웨어입니다. 권리 읽기(K)

읽지 않은 메일: 0개 전체: 1개

[Test mail 발송]

→

[Test mail 수신]

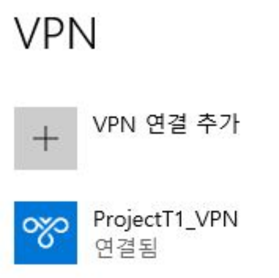
제목	글 쓴 사람	날짜
HELLO!	→ ksj@projectt1.net	오후 2:10

보낸 사람 나 <jinhee@projectt1.net>
제목 HELLO!
받는 사람 나 <ksj@projectt1.net>
오후 2:10

TEST MAIL

읽지 않은 메일: 0개 전체: 1개

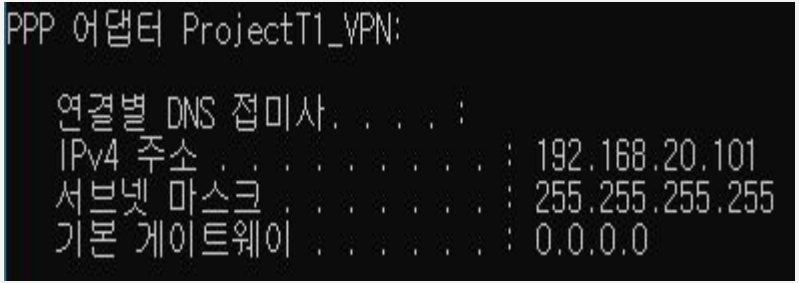
VPN



VPN

VPN 연결 추가

ProjectT1_VPN
연결됨



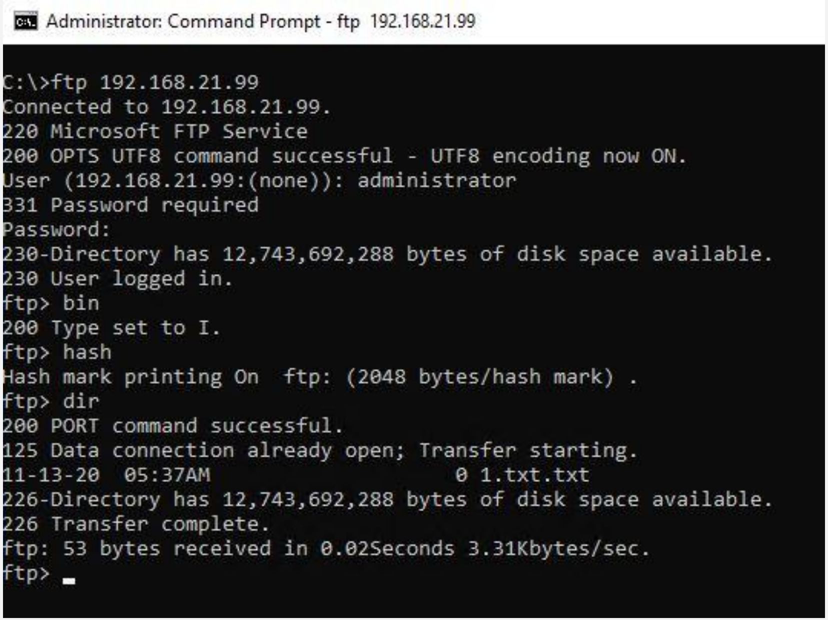
```
PPP 어댑터 ProjectT1_VPN:

   연결별 DNS 접미사. . . . :
   IPv4 주소 . . . . . . . . . : 192.168.20.101
   서브넷 마스크 . . . . . . . : 255.255.255.255
   기본 게이트웨이 . . . . . . : 0.0.0.0
```

VPN

- Type : L2TP
- 대역대 : 192.168.20.[100~200]
- 사내 Pirvate 영역 접근 가능

FTP

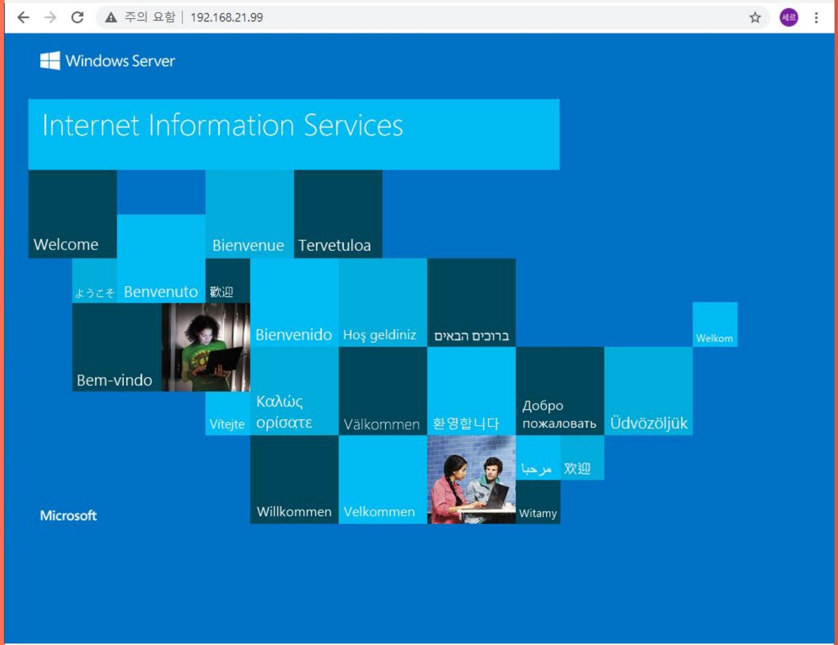


```
C:\>ftp 192.168.21.99
Connected to 192.168.21.99.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.21.99:(none)): administrator
331 Password required
Password:
230-Directory has 12,743,692,288 bytes of disk space available.
230 User logged in.
ftp> bin
200 Type set to I.
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-13-20  05:37AM                    0 1.txt.txt
226-Directory has 12,743,692,288 bytes of disk space available.
226 Transfer complete.
ftp: 53 bytes received in 0.02Seconds 3.31Kbytes/sec.
ftp> _
```

FTP

- 사내 FTP Server
- 외부 접근 불가능

HTTP



사내용 HTTP

- 사내 전용 Web Server
- VPN을 통해서만 접근 가능

Thanks!

김성주
sjk4425@naver.com

서진희
lillii9089@naver.com