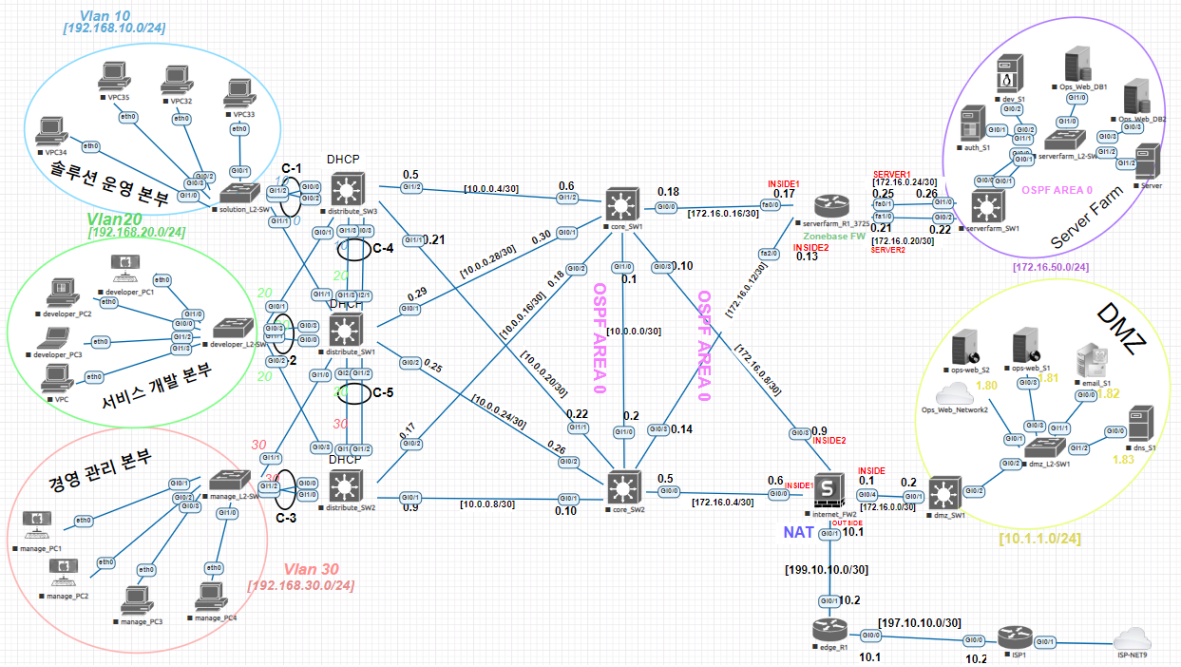
새둘(주) - 장비설정 기술문서

🌐 새둘(주) - 본사 네트워크



🌕 네트워크 엔터프라이즈

💠 Core SW

3️⃣ ↔ Core_SW1

```
01. L3 인터페이스 구성 및 라우팅 설정
ip routing
!
int g1/0
no sw
ip add 10.0.0.1 255.255.255.252
no sh
!
int g1/2
no sw
ip add 10.0.0.6 255.255.255.252
no sh
!
int g0/2
no sw
ip add 10.0.0.18 255.255.255.252
no sh
!
int g0/1
no sw
ip add 10.0.0.30 255.255.255.252
no sh
!
router ospf 10
network 10.0.0.1 0.0.0.0 area 0
network 10.0.0.6 0.0.0.0 area 0
network 10.0.0.18 0.0.0.0 area 0
network 10.0.0.30 0.0.0.0 area 0
!
```

3️⃣ ↔ Core_SW2

```
01. L3 인터페이스 구성 및 라우팅 설정
ip routing
!
int g1/0
no sw
ip add 10.0.0.2 255.255.255.252
no sh
!
int g0/1
no sw
ip add 10.0.0.10 255.255.255.252
no sh
!
int g1/1
no sw
ip add 10.0.0.22 255.255.255.252
no sh
!
int g0/2
no sw
ip add 10.0.0.26 255.255.255.252
no sh
!
router ospf 10
network 10.0.0.2 0.0.0.0 area 0
network 10.0.0.10 0.0.0.0 area 0
network 10.0.0.22 0.0.0.0 area 0
network 10.0.0.26 0.0.0.0 area 0
!
```

🔴🔵 HQ_VPN

```
en
conf t
!
int g0/0
ip add 172.16.0.13 255.255.255.0
no sh
!
int g0/1
ip add 10.10.12.2 255.255.255.0
no sh
!
int g0/2
ip add 10.10.23.1 255.255.255.0
no sh
!
router eigrp 10
network 10.0.0.0
!
router ospf 10
network 172.16.0.13 0.0.0.0 area 0
! 1. mGRE 설정
int tunnel 0
ip add 10.100.1.1 255.255.255.0
tunnel source 172.16.0.13
tunnel mode gre multipoint
tunnel key 10
! 2. nhrp 설정
ip nhrp authentication cisco
ip nhrp network-id 10
ip nhrp holdtime 600
ip nhrp map multicast dynamic
no ip next-hop eigrp 10
crypto isakmp policy 10
authentication pre-share
encryption aes
exit
! 3. ipsec 및 crypto profile 설정
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto ipsec transform-set ts_HQ->Branch esp-aes esp-sha-hmac
mode transport
crypto ipsec profile pf_HQ_Branch_VPN
set transform-set ts_HQ->Branch
int tunnel 0
tunnel protection ipsec profile pf_HQ_Branch_VPN
!
```

💠 Distribute SW

3️⃣↔ distribute_SW1

```
!-- distribute_SW1(개발)
en
conf t

01. vlan 10, 20, 30 생성
vlan 10
vlan 20
vlan 30
exit
!

02. vlan 멤버 추가
int range g0/0, g0/3
sw mo ac
sw ac vla 20
no sh
exit
!
int g1/1
sw mo ac
sw ac vla 10
no sh
exit
!
int g1/0
sw mo ac
sw ac vla 30
no sh
exit
!
int range g1/3, g2/1
sw tr en do
sw mo tr
sw tr al vl 10,20
sw tr na vl 99
sw non
no sh
exit
!
int range g1/2, g2/0
sw tr en do
sw mo tr
sw tr al vl 20,30
sw tr na vl 99
sw non
no sh
exit
!

03. STP 확인 조정
spanning-tree mode pvst
spanning-tree vlan 20 root primary
spanning-tree vlan 10 root secondary
spanning-tree vlan 30 root secondary
!

04. InterVlan Routing 설정
int vlan 10
ip add 192.168.10.253 255.255.255.0
no sh
exit
!
int vlan 20
ip add 192.168.20.254 255.255.255.0
no sh
exit
!
int vlan 30
ip add 192.168.30.253 255.255.255.0
no sh
exit
!

05. 이더 채널 구성
int range g0/0, g0/3
channel-group 2 mode desirable
!
int range g1/3, g2/1
channel-group 4 mode desirable
!
int range g1/2, g2/0
channel-group 5 mode desirable
!

06. HSRP 설정
int vlan 20
standby 20 ip 192.168.20.251
standby 20 priority 110
standby 20 preempt
standby 20 authentication 1qaz@wsx
standby version 2
exit
!
int vlan 10
standby 10 ip 192.168.10.251
standby 10 priority 90
standby 10 preempt
standby 10 authentication 1qaz@wsx
standby version 2
exit
!
int vlan 30
standby 30 ip 192.168.30.251
standby 30 priority 90
standby 30 preempt
standby 30 authentication 1qaz@wsx
standby version 2

07. DHCP 설정
ip dhcp excluded-address 192.168.20.1 192.168.20.20
ip dhcp pool solution
network 192.168.20.0 255.255.255.0
default-router 192.168.20.251
dns-server 8.8.8.8
lease 7 0 0
```

3️⃣↔ distribute_SW2

```
!-- distribute_SW2(경영관리)
en
conf t

01. vlan 20, 30 생성
vlan 20
vlan 30
exit
!

02. vlan 멤버 추가
int range g0/0, g1/0
sw mo ac
sw ac vla 30
no sh
exit
!
int g0/3
sw mo ac
sw ac vla 20
no sh
exit
!
int range g1/1 - 2
sw tr en do
sw mo tr
sw tr al vl 20,30
sw tr na vl 99
sw non
no sh
exit
!

03. STP 확인 조정
spanning-tree mode pvst
spanning-tree vlan 30 root primary
spanning-tree vlan 20 root secondary
!

04. InterVlan Routing 설정
int vlan 20
ip add 192.168.20.253 255.255.255.0
no sh
exit
!
int vlan 30
ip add 192.168.30.254 255.255.255.0
no sh
exit
!

05. 이더 채널 구성
int range g0/0, g1/0
channel-group 3 mode desirable
!
int range g1/1 - 2
channel-group 5 mode desirable
!

06. HSRP 설정
int vlan 10
standby 10 ip 192.168.10.251
standby 10 priority 90
standby 10 preempt
standby 10 authentication 1qaz@wsx
standby version 2
exit
!
int vlan 30
standby 30 ip 192.168.30.251
standby 30 priority 110
standby 30 preempt
standby 30 authentication 1qaz@wsx
standby version 2

07. DHCP 설정
ip dhcp excluded-address 192.168.30.1 192.168.30.20
ip dhcp pool design
network 192.168.30.0 255.255.255.0
default-router 192.168.30.251
dns-server 8.8.8.8
lease 7 0 0
!

08. OSPF 설정
int g0/1
no sw
ip add 10.0.0.9 255.255.255.252
no sh
!
int g0/2
no sw
ip add 10.0.0.17 255.255.255.252
no sh
!
router ospf 10
network 10.0.0.9 0.0.0.0 area 0
network 10.0.0.17 0.0.0.0 area 0
network 192.168.30.254 0.0.0.0 area 0
network 192.168.20.253 0.0.0.0 area 0
!
```

3️⃣↔ distribute_SW3

```
!-- distribute_SW3(솔루션)
en
conf t

01. vlan 10, 20 생성
vlan 10
vlan 20
exit
!

02. vlan 멤버 추가
int range g0/0, g0/2
sw mo ac
sw ac vla 10
no sh
exit
!
int g0/1
sw mo ac
sw ac vla 20
no sh
exit
!
int range g0/3, g1/3
sw tr en do
sw mo tr
sw tr al vl 10,20
sw tr na vl 99
sw non
no sh
exit
!

03. STP 확인 조정
spanning-tree mode pvst
spanning-tree vlan 10 root primary
spanning-tree vlan 20 root secondary
!

04. InterVlan Routing 설정
int vlan 10
ip add 192.168.10.254 255.255.255.0
no sh
exit
!
int vlan 20
ip add 192.168.20.252 255.255.255.0
no sh
exit
!

05. 이더 채널 구성
int range g0/0, g0/2
channel-group 1 mode desirable
!
int range g0/3, g1/3
channel-group 4 mode desirable
!

06. HSRP 설정
int vlan 10
standby 10 ip 192.168.10.251
standby 10 priority 110
standby 10 preempt
standby 10 authentication 1qaz@wsx
standby version 2
exit
!
int vlan 20
standby 20 ip 192.168.20.251
standby 20 priority 90
standby 20 preempt
standby 20 authentication 1qaz@wsx
standby version 2

07. DHCP 설정
ip dhcp excluded-address 192.168.10.1 192.168.10.20
ip dhcp pool manage
network 192.168.10.0 255.255.255.0
default-router 192.168.10.251
dns-server 8.8.8.8
lease 7 0 0
!

08. OSPF 설정
int g1/1
no sw
ip add 10.0.0.21 255.255.255.252
no sh
!
int g1/2
no sw
ip add 10.0.0.5 255.255.255.252
no sh
!
router ospf 10
network 10.0.0.21 0.0.0.0 area 0
network 10.0.0.5 0.0.0.0 area 0
network 192.168.10.254 0.0.0.0 area 0
network 192.168.20.252 0.0.0.0 area 0
!
```

```
!

08. OSPF 설정
int g0/1
no sw
ip add 10.0.0.29 255.255.255.252
no sh
!
int g0/2
no sw
ip add 10.0.0.25 255.255.255.252
no sh
!
router ospf 10
network 10.0.0.29 0.0.0.0 area 0
network 10.0.0.25 0.0.0.0 area 0
network 192.168.20.254 0.0.0.0 area 0
network 192.168.10.253 0.0.0.0 area 0
network 192.168.30.253 0.0.0.0 area 0
!
```

💠 Access SW

2️⃣↔ L2_SW_solution

```
01. VLAN 10 생성
vlan 10
exit
!

02. VLAN 멤버 추가
int range g0/0 - 3, g1/0 - 2
sw mo ac
sw ac vla 10
no sh
exit
!

03. STP 설정
spanning-tree mode pvst
!

04. 이더 채널 구성
int range g0/0, g1/2
channel-group 1 mode desirable
!

05. AAA 설정
aaa new-model
!
tacacs server TACACS
add ipv4 192.168.10.100
key cisco
single-connection
!
aaa authentication login Authen group tacacs+
aaa authorization exec Author group tacacs+
aaa accounting exec Account_exec start-stop group tacacs+
aaa accounting commands 15 Account_commands start-stop group tacacs+
!
line vty 0 4
transport input ssh
login authentication Authen
authorization exec Author
accounting commands 15 Account_commands
accounting exec Account_exec
exit
!
```

2️⃣↔ L2_SW_developer

```
01. VLAN 20 생성
vlan 20
exit
!

02. VLAN 멤버 추가
int range g0/0 - 3, g1/0 - 3
sw mo ac
sw ac vla 20
no sh
exit
!

03. STP 설정
spanning-tree mode pvst
!

04. 이더 채널 구성
int range g0/3, g1/1
channel-group 2 mode desirable
!
```

2️⃣↔ L2_SW_manage

```
01. VLAN 30 생성
vlan 30
exit
!

02. VLAN 멤버 추가
int range g0/0 - 3, g1/0 - 2
sw mo ac
sw ac vla 30
no sh
exit
!

03. STP 설정
spanning-tree mode pvst
!

04. 이더 채널 구성
int range g0/0, g1/2
channel-group 3 mode desirable
!
```

💠 HOST

💻 design_PC1-4 :: solution_PC1-4 :: manage_PC1-4

```
ip dhcp -r
```

🌕 네트워크 도입부 및 DMZ

💠 Outside

✴️ edge_R1

```
!--IOS BASIC CONFIG
hostname edge_R1
!
enable secret cisco
!
ip domain-name yycloud.net
!
no ip domain-lookup
!
banner motd ^
This is a edge_R1
^
!
username user01 secret cisco
username admin privilege 15 secret cisco
!
ip ssh version 2
ip ssh time-out 30
crypto key generate rsa general-keys modulus 1024
!
line con 0
 exec-timeout 0
 logging sync
```

✴️ ISP1

```
!-- ISP1 Router Basic Config
hostname ISP1
!
enable secret cisco
!
ip domain-name yycloud.net
!
no ip domain-lookup
!
banner motd ^
This is a ISP1 Router.
^
!
username user01 secret cisco
username admin privilege 15 secret cisco
!
ip ssh version 2
ip ssh time-out 30
crypto key generate rsa general-keys modulus 1024
!
line con 0
 exec-timeout 0
 logging sync
```

```
 login local
 exit
!
line vty 0 4
  exec-timeout 0
  logging sync
  transport  input ssh
  login local
  exit
!
!-- INTERFACE IP CONFIG
!
int g0/0
  ip add 197.10.10.1 255.255.255.252
  no sh
  exit
int g0/1
  ip add 199.10.10.2 255.255.255.252
  no sh
  exit
int g0/2
  ip add 198.10.10.1 255.255.255.252
  no sh
  exit
!
!-- Static Routing Config
ip route 172.16.0.0 255.255.255.252 g0/1 199.10.10.1
ip route 10.1.1.0 255.255.255.0 g0/1 199.10.10.1
!
```

```
 login local
 exit
!
line vty 0 4
  exec-timeout 0
  logging sync
  transport input ssh
  login local
  exit
!
!-- IP 설정
int g0/0
  ip add 197.10.10.2 255.255.255.252
  no sh
  exit
int g0/1
  ip add dhcp
  no sh
  exit
!
!-- Static Routing 설정
ip route 10.1.1.0 255.255.255.0 g0/0 197.10.10.1
ip route 172.16.0.0 255.255.255.252 g0/0 197.10.10.1
ip route 198.10.10.0 255.255.255.252 g0/0 197.10.10.1
ip route 199.10.10.0 255.255.255.252 g0/0 197.10.10.1
```

💠 DMZ

2️⃣↔ dmz_L2_SW1

```
!-- L2 Switch Basic Config
hostname dmz_L2SW1
!
enable secret cisco
!
ip domain-name yycloud.net
!
no ip domain-lookup
!
banner motd ^
This is a dmz_L2SW1 L2 switch.
^
!
username user01 secret cisco
username admin privilege 15 secret cisco
!
ip ssh version 2
ip ssh time-out 30
crypto key generate rsa general-keys modulus 1024
!
line con 0
 exec-timeout 0
 logging sync
 login local
 exit
!
line vty 0 4
  exec-timeout 0
  logging sync
  transport input ssh
  login local
  exit
!
```

4️⃣ dmz_R1

```
!-- dmz_R1 Router Basic Config
hostname dmz_R1
!
enable secret cisco
!
ip domain-name yycloud.net
!
no ip domain-lookup
!
banner motd ^
This is a dmz_R1 router.
^
!
username user01 secret cisco
username admin privilege 15 secret cisco
!
ip ssh version 2
ip ssh time-out 30
crypto key generate rsa general-keys modulus 1024
!
line con 0
 exec-timeout 0
 logging sync
 login local
 exit
!
line vty 0 4
  exec-timeout 0
  logging sync
  transport input ssh
  login local
  exit
!
!-- 인터페이스 설정
int g0/1
  ip add 172.16.0.2 255.255.255.0
  no sh
  exit
int g0/2
  ip add 10.1.1.254 255.255.255.0
  no sh
  exit
!
!-- OSPF 설정
!
router ospf 50
  network 10.1.1.254 0.0.0.0 area 0
  network 172.16.0.2 0.0.0.0 area 0
!
!-- 기본 게이트웨이 설정
ip default-gateway 172.16.0.1
```

🌎 dns_S1

```
!-- IOS Basic Config
hostname dns_S1
!
enable secret cisco
!
ip domain-name yycloud.net
!
no ip domain-lookup
!
banner motd ^
This is a dns_S1 router.
^
!
username user01 secret cisco
username admin privilege 15 secret cisco
!
ip ssh version 2
ip ssh time-out 30
crypto key generate rsa general-keys modulus 1024
!
line con 0
 exec-timeout 0
 logging sync
 login local
 exit
```

🌎 email_S1

```
!-- IOS Basic Config
hostname email_S1
!
enable secret cisco
!
ip domain-name yycloud.net
!
no ip domain-lookup
!
banner motd ^
This is a email_S1 router.
^
!
username user01 secret cisco
username admin privilege 15 secret cisco
!
ip ssh version 2
ip ssh time-out 30
crypto key generate rsa general-keys modulus 1024
!
line con 0
 exec-timeout 0
 logging sync
 login local
 exit
```

```
!
line vty 0 4
  exec-timeout 0
  logging sync
  transport input ssh
  login local
  exit
!
!-- IP 및 라우팅 테이블 설정
int g0/0
  ip add 10.1.1.83 255.255.255.0
  no sh
  exit
!
ip route 0.0.0.0 0.0.0.0 g0/0 10.1.1.254
!
```

```
!
line vty 0 4
  exec-timeout 0
  logging sync
  transport input ssh
  login local
  exit
!
!-- IP 및 라우팅 테이블 설정
int g0/0
  ip add 10.1.1.82 255.255.255.0
  no sh
  exit
!
ip route 0.0.0.0 0.0.0.0 g0/0 10.1.1.254
!
```

🌎 ops-web_S1

```
!-- IOS Basic Config
hostname ops-web_S1
!
enable secret cisco
!
ip domain-name yycloud.net
!
no ip domain-lookup
!
banner motd ^
This is a ops-web_S1 router.
^
!
username user01 secret cisco
username admin privilege 15 secret cisco
!
ip ssh version 2
ip ssh time-out 30
crypto key generate rsa general-keys modulus 1024
!
line con 0
 exec-timeout 0
 logging sync
 login local
 exit
!
line vty 0 4
  exec-timeout 0
  logging sync
  transport input ssh
  login local
  exit
!
!-- IP 및 라우팅 테이블 설정
int g0/3
  ip add 10.1.1.81 255.255.255.0
  no sh
  exit
!
ip route 0.0.0.0 0.0.0.0 g0/3 10.1.1.254
!
!-- Web Server On
ip http server
```

🌎 ops-web_S2

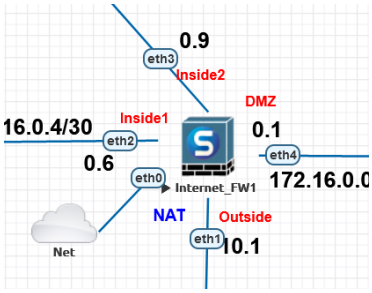
```
!-- IOS Basic Config
hostname ops-web_S2
!
enable secret cisco
!
ip domain-name yycloud.net
!
no ip domain-lookup
!
banner motd ^
This is a ops-web_S2 router.
^
!
username user01 secret cisco
username admin privilege 15 secret cisco
!
ip ssh version 2
ip ssh time-out 30
crypto key generate rsa general-keys modulus 1024
!
line con 0
 exec-timeout 0
 logging sync
 login local
 exit
!
line vty 0 4
  exec-timeout 0
  logging sync
  transport input ssh
  login local
  exit
!
!-- IP 및 라우팅 테이블 설정
int g0/0
  ip add 10.1.1.80 255.255.255.0
  no sh
  exit
!
ip route 0.0.0.0 0.0.0.0 g0/0 10.1.1.254
!
!-- Web Server On
ip http server
```

💠 FireWall

🧱 Internet_FW1 (ACL)

```
!-- 1. IOS 방화벽 기본설정
!
hostname Internet_FW1
!
enable secret cisco
!
ip domain-name yycloud.net
!
no ip domain-lookup
!
banner motd ^
This is a Internet_FW1 router.
^
!
username user01 secret cisco
username admin privilege 15 secret cisco
!
ip ssh version 2
ip ssh time-out 30
crypto key generate rsa general-keys modulus 1024
!
line con 0
 exec-timeout 0
 logging sync
 login local
 exit
!
line vty 0 4
  exec-timeout 0
  logging sync
  transport input ssh
  login local
  exit
!
!-- 2. 인터페이스 설정(검사 규칙 및 ACL 적용도 포함)
interface GigabitEthernet0/1
 ip address 199.10.10.1 255.255.255.252
 ip access-group OUT_ACL in
!
interface GigabitEthernet0/4
 ip address 172.16.0.1 255.255.255.252
 ip access-group DMZ_ACL in
 ip inspect FWRULE in
!
!-- 3. 방화벽 정적 라우팅 설정
```

🧱 Internet_FW1 (sophos)



인터페이스

구역 이름	소포스 인터페이스	도면 인터페이스	인터페이스 IP
OUTSIDE	eth1	g0/1	199.10.10.1/30
INSIDE 1	eth2	g0/0	172.16.0.6/30
INSIDE 2	eth3	g0/3	172.16.0.9/30
DMZ	eth4	g0/4	172.16.0.1/30

💡 Sophos UTM 노드에서 eth 0은 관리 목적으로 사용하며,
https://192.168.3.118:4444 로 관리

정책

Sources	Services	Destinations	Action

```
ip route 10.1.1.0 255.255.255.0 GigabitEthernet0/4
ip route 197.10.10.0 255.255.255.252 GigabitEthernet0/1
ip route 198.10.10.0 255.255.255.252 GigabitEthernet0/1
!
!-- 4. 감사추적 및 실시간 경보 활성화
!
logging on
logging host 10.0.0.3
ip inspect audit-trail
no ip inspect alert-off
!
!-- 5. 검사 규칙 설정
ip inspect name FWRULE https alert on audit-trail on timeout 300
ip inspect name FWRULE http alert on audit-trail on timeout 300
ip inspect name FWRULE dns alert on audit-trail on timeout 300
ip inspect name FWRULE smtp alert on audit-trail on timeout 300
ip inspect name FWRULE pop3 alert on audit-trail on timeout 300
ip inspect name FWRULE pop3s alert on audit-trail on timeout 300
ip inspect name FWRULE imap alert on audit-trail on timeout 300
ip inspect name FWRULE imap3 alert on audit-trail on timeout 300
ip inspect name FWRULE imaps alert on audit-trail on timeout 300
ip inspect name FWRULE icmp alert on audit-trail on timeout 300
ip inspect name FWRULE tcp alert on audit-trail on timeout 300
ip inspect name FWRULE udp alert on audit-trail on timeout 300
!
!-- 6. ACL 설정
!
ip access-list extended DMZ_ACL
 permit icmp any any packet-too-big
 permit udp any any
 permit tcp any any
 permit ip any any
ip access-list extended OUT_ACL
 permit tcp any host 10.1.1.82 eq smtp
 permit tcp any host 10.1.1.82 eq pop3
 permit tcp any host 10.1.1.81 eq 443
 permit tcp any host 10.1.1.81 eq www
 permit tcp any host 10.1.1.82 eq 220
 permit udp any host 10.1.1.83 eq domain
 permit icmp any any packet-too-big
 permit ip any any log
!
```

Sources	Services	Destinations	Action
OUTSIDE(Network)	HTTPS, SSH, VPN Protocols	DMZ(Network)	Allow
DMZ(Network)	MySQL	INSIDE(Network)	Allow
DMZ(Network)	HTTPS	INSIDE(Network)	Drop
INSIDE(Network)	HTTPS, SSH	OUTSIDE(Network)	Allow
OUTSIDE(Network)	HTTPS, SSH	INSIDE(Network)	Allow

💡 INSIDE1 및 INSIDE2는 같은 INSIDE로 간주

StaticRouting 설정

Route Type	대상 Network	출발 Interface
Interface	10.1.1.0/24	DMZ
Interface	197.10.10.0/30	OUTSIDE
Interface	198.10.10.0/30	OUTSIDE

OSPF 설정

- interface

OSPF 인터페이스	사용 인터페이스
OUTSIDE_OSPF	eth1
INSIDE1_OSPF	eth2
INSIDE2_OSPF	eth3
INSIDE_OSPF	eth4

- Area

area-id	0.0.0.0
connect-vid-interface	OUTSIDE_OSPF, INSIDE1_OSPF, INSIDE2_OSPF, INSIDE_OSPF

- Global

Router-id	172.16.0.0

🌕 SERVER_FARM

3️⃣↔ serverfarm_SW1

```
!--IOS BASIC CONFIG
hostname serverfarm_SW1
!
enable secret cisco
!
ip domain-name yycloud.net
!
no ip domain-lookup
!
banner motd ^
This is serverfarm_SW1
^
!
username user01 secret cisco
username admin privilege 15 secret cisco
!
ip ssh version 2
ip ssh time-out 30
crypto key generate rsa general-keys modulus 1024
!
line con 0
 exec-timeout 0
 logging sync
 login local
 exit
!
line vty 0 4
  exec-timeout 0
  logging sync
  transport  input ssh
  login local
  exit
!
!-- INTERFACE IP CONFIG
int g1/0
no switchport
ip add 172.16.0.22 255.255.255.252
no sh
!
int g0/1
no switchport
ip add 172.16.50.254 255.255.255.0
no sh
!
!-- PORT CHANNEL SETTING
!--int port-channel 16
!--no switchport
!--ip add 172.16.0.22 255.255.255.252
!--exit
!
!--int g1/0
```

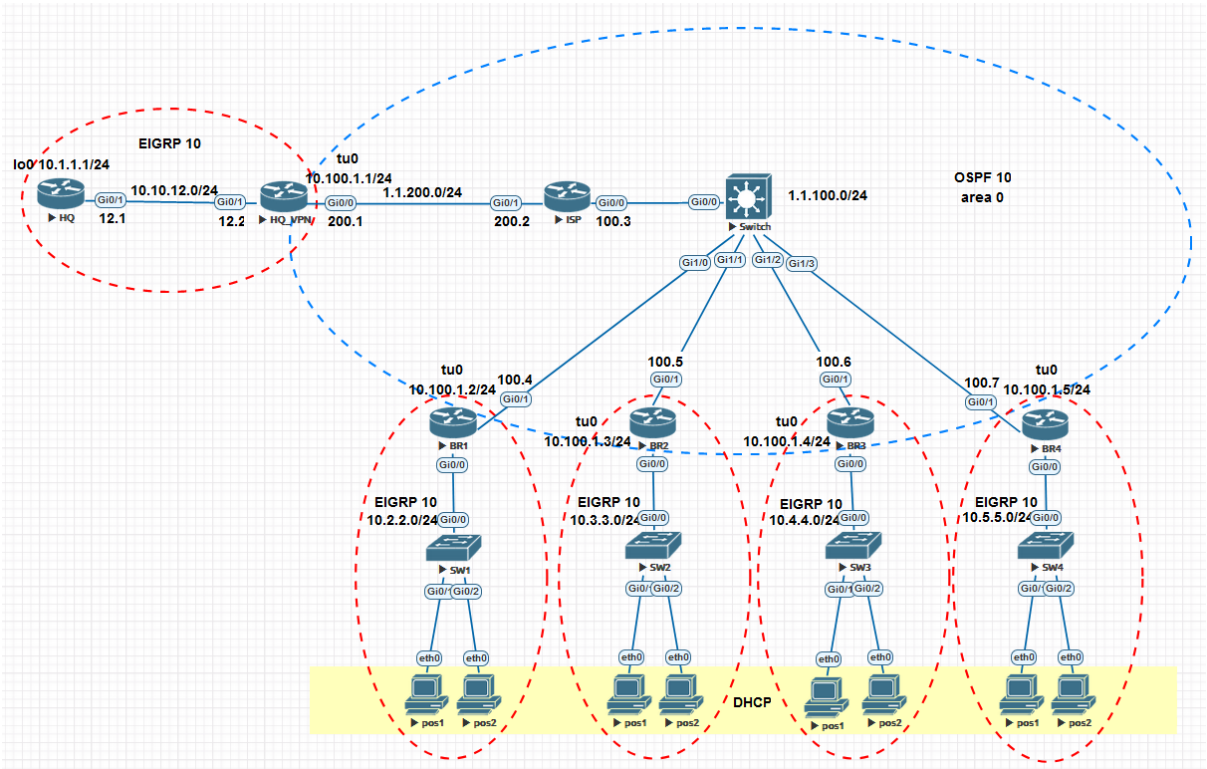
🧱✳️ serverfarm_R1 (Zonebase FW)

```
!--IOS BASIC CONFIG
hostname serverfarm_R
!
enable secret cisco
!
ip domain-name yycloud.net
!
no ip domain-lookup
!
banner motd ^
This is a serverfarm_R1
^
!
username user01 secret cisco
username admin privilege 15 secret cisco
!
ip ssh version 2
ip ssh time-out 30
crypto key generate rsa general-keys modulus 1024
!
line con 0
 exec-timeout 0
 logging sync
 login local
 exit
!
line vty 0 4
  exec-timeout 0
  logging sync
  transport  input ssh
  login local
  exit
!
!-- INTERFACE IP CONFIG----------------------------------------------------------------------
!-- INSIDE2
int f2/0
ip add 172.16.0.13 255.255.255.252
no sh
!
!-- INSIDE1
int f0/0
ip add 172.16.0.17 255.255.255.252
no sh
!
!-- SERVER1
int f0/1
ip add 172.16.0.21 255.255.255.252
no sh
!
!-- SERVER2
!-- int f1/0
```

```
!--no switchport
!--channel-group 16 mode desirable
!--int g0/2
!--no switchport
!--channel-group 16 mode desirable
!--do sh etherchannel summary
!
!-- OSPF
router ospf 100
network 172.16.0.22 0.0.0.0 area 0
network 172.16.50.254 0.0.0.0 area 0
```

```
!-- ip add 172.16.0.21 255.255.255.252
!-- no sh
!-- exit
!
!-- ZONE SETTING----------------------------------------------------------------------------
zone security INSIDE1
exit
zone security INSIDE2
exit
zone security SERVER1
exit
zone security SERVER2
exit
!-- ZONE SETTING TO INTERFACE
int f0/0
zone-member security INSIDE1
int f2/0
zone-member security INSIDE2
int f0/1
zone-member security SERVER1
int f1/0
zone-member security SERVER2
do show zone security
!-- Access-Rule
!-- INSIDE1 -> SERVER1
!-- INSIDE2 -> SERVER2
!-- SERVER1 -> INSIDE
!
!-- PORT CHANNEL SETTING
!--int port-channel 16
!--ip add 172.16.0.21 255.255.255.252
!--exit
!
!--int f1/0
!--channel-group 16
!-- int f0/1
!-- channel-group 16 mode desirable
!-- do sh etherchannel summary
!
!-- OSPF
router ospf 100
network 172.16.0.21 0.0.0.0 area 0
network 172.16.0.13 0.0.0.0 area 0
network 172.16.0.17 0.0.0.0 area 0
```

🌐 새둘(주) - 지사 네트워크



🌕 네트워크 도입부

🚨✳️ HQ_VPN (config-1)

```
HQ_VPN(config-if)#int g0/0
HQ_VPN(config-if)#ip add 1.1.200.1 255.255.255.0
HQ_VPN(config-if)#no sh
HQ_VPN(config)#int g0/1
HQ_VPN(config-if)#ip add 10.10.12.2 255.255.255.0
HQ_VPN(config-if)#no sh
HQ_VPN(config)#ip route 0.0.0.0 0.0.0.0 g0/0 1.1.200.2
HQ_VPN(config)#router ospf 10
HQ_VPN(config-router)#network 1.1.200.1 0.0.0.0 area 0
```

🚨✳️ HQ_VPN (config-2)

```
hostname HQ_VPN

crypto isakmp policy 10
encr aes
authentication pre-share
crypto isakmp key cisco address 0.0.0.0

crypto ipsec transform-set ts_HQ->Branch esp-aes esp-sha-hmac
```

```
HQ_VPN(config)#router eigrp 10
HQ_VPN(config-router)#no auto-summary
HQ_VPN(config-router)#network 10.10.12.2 0.0.0.0
HQ_VPN(config-router)#network 10.100.1.1 0.0.0.0
HQ_VPN(config)#int tunnel 0
HQ_VPN(config-if)#no ip split-horizon eigrp 10
HQ_VPN(config)#int tunnel 0
HQ_VPN(config-if)#ip add 10.100.1.1 255.255.255.0
HQ_VPN(config-if)#ip nhrp authentication cisco
HQ_VPN(config-if)#tunnel source 1.1.200.1
HQ_VPN(config-if)#tunnel mode gre multipoint
HQ_VPN(config-if)#tunnel key 10
HQ_VPN(config-if)#ip nhrp network-id 10
HQ_VPN(config-if)#ip nhrp holdtime 600
HQ_VPN(config-if)#ip nhrp map multicast dynamic
HQ_VPN(config-if)#no ip next-hop eigrp 10
HQ_VPN(config)#crypto isakmp policy 10
HQ_VPN(config-isakmp)#authentication pre-share
HQ_VPN(config-isakmp)#encryption aes
HQ_VPN(config-isakmp)#exit
HQ_VPN(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0
HQ_VPN(config)#crypto ipsec transform-set ts_HQ->Branch esp-aes esp-sha-hmac
HQ_VPN(cfg-crypto-trans)#mode transport
HQ_VPN(config)#crypto ipsec profile pf_HQ_Branch_VPN
HQ_VPN(ipsec-profile)#set transform-set ts_HQ->Branch
HQ_VPN(ipsec-profile)#int tunnel 0
HQ_VPN(config-if)#tunnel protection ipsec profile pf_HQ_Branch_VPN
```

✳️ ISP

```
ISP(config)#int g0/0
ISP(config-if)#ip add 1.1.100.2 255.255.255.0
ISP(config-if)#no sh
ISP(config-if)#int g0/1
ISP(config-if)#ip add 1.1.200.2 255.255.255.0
ISP(config-if)#no sh
ISP(config-if)#int g0/0
ISP(config-if)#ip add 1.1.100.3 255.255.255.0
ISP(config-if)#no sh
ISP(config)#router ospf 10
ISP(config-router)#network 1.1.100.3 0.0.0.0 area 0
ISP(config-router)#network 1.1.200.2 0.0.0.0 area 0
```

```
crypto ipsec profile pf_HQ_Branch_VPN
 set transform-set ts_HQ->Branch

interface Tunnel0
 ip address 10.100.1.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 10
 ip nhrp holdtime 600
 tunnel source 172.16.0.13
 tunnel mode gre multipoint
 tunnel key 10
 tunnel protection ipsec profile pf_HQ_Branch_VPN
!

interface GigabitEthernet0/0
 ip address 172.16.0.13 255.255.255.0

interface GigabitEthernet0/1
 ip address 10.10.12.2 255.255.255.0

interface GigabitEthernet0/2
 ip address 10.10.23.1 255.255.255.0

router eigrp 10
 network 10.0.0.0
!
router ospf 10
 network 172.16.0.13 0.0.0.0 area 0
!

int tunnel 0
tunnel protection ipsec profile pf_HQ_Branch_VPN

router eigrp 10
no auto-summary

int tunnel 0
no ip split-horizon eigrp 10
```

✳️ HQ

```
HQ(config)#int g0/1
HQ(config-if)#ip add 10.10.12.1 255.255.255.0
HQ(config-if)#no sh
HQ(config-if)#int lo0
HQ(config-if)#ip add 10.1.1.1 255.255.255.
HQ(config)#router eigrp 10
HQ(config-router)#no auto-summary
HQ(config-router)#network 10.10.12.1 0.0.0.0
HQ(config-router)#network 10.1.1.1 0.0.0.0
```

🌕 지사 네트워크 엔터프라이즈

💠 Branch

✳️ BR1

```
!-- 기본 설정
Router>en
Router#conf t
Router(config)#host BR1
BR1(config)#no ip domain-lookup
BR1(config)#line con 0
BR1(config-line)#exec-timeout 0
BR1(config-line)#logging sync

!-- 인터페이스 설정
BR1(config)#int g0/0
BR1(config-if)#ip add 10.2.2.254 255.255.255.0
BR1(config-if)#no sh
BR1(config-if)#int g0/1
BR1(config-if)#ip add 1.1.100.4 255.255.255.0
BR1(config-if)#no sh

!-- OSPF 설정
BR1(config)#router ospf 10
BR1(config-router)#network 1.1.100.4 0.0.0.0 area 0

!-- EIGRP 설정
BR1(config)#router eigrp 10
BR1(config-router)#no auto-summary
BR1(config-router)#network 10.2.2.254 0.0.0.0
BR1(config-router)#network 10.100.1.2 0.0.0.0

!-- mGRE 설정
BR1(config)#int tunnel 0
BR1(config-if)#ip address 10.100.1.2 255.255.255.0
BR1(config-if)#ip nhrp authentication cisco
BR1(config-if)#tunnel source 1.1.100.4
BR1(config-if)#tunnel mode gre multipoint
BR1(config-if)#tunnel key 10

!-- NHRP 설정
BR1(config-if)#ip nhrp network-id 10
BR1(config-if)#ip nhrp nhs 10.100.1.1
BR1(config-if)#ip nhrp map 10.100.1.1 1.1.200.1
BR1(config-if)#ip nhrp map multicast 1.1.200.1
BR1(config-if)#ip nhrp registration timeout 60

!-- IPSec 설정
BR1(config)#crypto isakmp policy 10
BR1(config-isakmp)#authentication pre-share
BR1(config-isakmp)#encr aes
BR1(config-isakmp)#exit
BR1(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0
BR1(config)#crypto ipsec transform-set ts_BR->HQ esp-aes esp-sha-hmac
BR1(cfg-crypto-trans)#mode transport
BR1(cfg-crypto-trans)#crypto ipsec profile pf_HQ_BR_VPN
BR1(ipsec-profile)#set transform-set ts_BR->HQ
```

✳️ BR2

```
!-- 기본 설정
Router>en
Router#conf t
Router(config)#host BR2
BR2(config)#no ip domain-lookup
BR2(config)#line con 0
BR2(config-line)#exec-timeout 0
BR2(config-line)#logging sync

!-- 인터페이스 설정
BR2(config)#int g0/0
BR2(config-if)#ip add 10.3.3.254 255.255.255.0
BR2(config-if)#no sh
BR2(config-if)#int g0/1
BR2(config-if)#ip add 1.1.100.5 255.255.255.0
BR2(config-if)#no sh

!-- OSPF 설정
BR2(config)#router ospf 10
BR2(config-router)#network 1.1.100.4 0.0.0.0 area 0

!-- EIGRP 설정
BR2(config)#router eigrp 10
BR2(config-router)#no auto-summary
BR2(config-router)#network 10.3.3.254 0.0.0.0
BR2(config-router)#network 10.100.1.3 0.0.0.0

!-- mGRE 설정
BR2(config)#int tunnel 0
BR2(config-if)#ip address 10.100.1.3 255.255.255.0
BR2(config-if)#ip nhrp authentication cisco
BR2(config-if)#tunnel source 1.1.100.5
BR2(config-if)#tunnel mode gre multipoint
BR2(config-if)#tunnel key 10

!-- NHRP 설정
BR2(config-if)#ip nhrp network-id 10
BR2(config-if)#ip nhrp nhs 10.100.1.1
BR2(config-if)#ip nhrp map 10.100.1.1 1.1.200.1
BR2(config-if)#ip nhrp map multicast 1.1.200.1
BR2(config-if)#ip nhrp registration timeout 60

!-- IPSec 설정
BR2(config)#crypto isakmp policy 10
BR2(config-isakmp)#authentication pre-share
BR2(config-isakmp)#encr aes
BR2(config-isakmp)#exit
BR2(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0
BR2(config)#crypto ipsec transform-set ts_BR->HQ esp-aes esp-sha-hmac
BR2(cfg-crypto-trans)#mode transport
BR2(cfg-crypto-trans)#crypto ipsec profile pf_HQ_BR_VPN
BR2(ipsec-profile)#set transform-set ts_BR->HQ
```

```
BR1(ipsec-profile)#exit
BR1(config)#int tunnel 0
BR1(config-if)#tunnel protection ipsec profile pf_HQ_BR_VPN

!-- DHCP 설정
BR1(config)#ip dhcp pool BR_pool
BR1(dhcp-config)#network 10.2.2.0 255.255.255.0
BR1(dhcp-config)#default-router 10.2.2.254
BR1(dhcp-config)#dns-server 8.8.8.8
BR1(dhcp-config)#lease infinite
BR1(dhcp-config)#exit
BR1(config)#ip dhcp excluded-address 10.2.2.101 10.2.2.254
```

```
BR2(ipsec-profile)#exit
BR2(config)#int tunnel 0
BR2(config-if)#tunnel protection ipsec profile pf_HQ_BR_VPN

!-- DHCP 설정
BR2(config)#ip dhcp pool BR_pool
BR2(dhcp-config)#network 10.3.3.0 255.255.255.0
BR2(dhcp-config)#default-router 10.3.3.254
BR2(dhcp-config)#dns-server 8.8.8.8
BR2(dhcp-config)#lease infinite
BR2(dhcp-config)#exit
BR2(config)#ip dhcp excluded-address 10.3.3.101 10.3.3.254
```

✳️ BR3

```
!-- 기본 설정
Router>en
Router#conf t
Router(config)#host BR3
BR3(config)#no ip domain-lookup
BR3(config)#line con 0
BR3(config-line)#exec-timeout 0
BR3(config-line)#logging sync

!-- 인터페이스 설정
BR3(config)#int g0/0
BR3(config-if)#ip add 10.4.4.254 255.255.255.0
BR3(config-if)#no sh
BR3(config-if)#int g0/1
BR3(config-if)#ip add 1.1.100.6 255.255.255.0
BR3(config-if)#no sh

!-- OSPF 설정
BR3(config)#router ospf 10
BR3(config-router)#network 1.1.100.6 0.0.0.0 area 0

!-- EIGRP 설정
BR3(config)#router eigrp 10
BR3(config-router)#no auto-summary
BR3(config-router)#network 10.4.4.254 0.0.0.0
BR3(config-router)#network 10.100.1.4 0.0.0.0

!-- mGRE 설정
BR3(config)#int tunnel 0
BR3(config-if)#ip address 10.100.1.4 255.255.255.0
BR3(config-if)#ip nhrp authentication cisco
BR3(config-if)#tunnel source 1.1.100.6
BR3(config-if)#tunnel mode gre multipoint
BR3(config-if)#tunnel key 10

!-- NHRP 설정
BR3(config-if)#ip nhrp network-id 10
BR3(config-if)#ip nhrp nhs 10.100.1.1
BR3(config-if)#ip nhrp map 10.100.1.1 1.1.200.1
BR3(config-if)#ip nhrp map multicast 1.1.200.1
BR3(config-if)#ip nhrp registration timeout 60

!-- IPSec 설정
BR3(config)#crypto isakmp policy 10
BR3(config-isakmp)#authentication pre-share
BR3(config-isakmp)#encr aes
BR3(config-isakmp)#exit
BR3(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0
BR3(config)#crypto ipsec transform-set ts_BR->HQ esp-aes esp-sha-hmac
BR3(cfg-crypto-trans)#mode transport
BR3(cfg-crypto-trans)#crypto ipsec profile pf_HQ_BR_VPN
BR3(ipsec-profile)#set transform-set ts_BR->HQ
BR3(ipsec-profile)#exit
BR3(config)#int tunnel 0
BR3(config-if)#tunnel protection ipsec profile pf_HQ_BR_VPN

!-- DHCP 설정
BR3(config)#ip dhcp pool BR_pool
BR3(dhcp-config)#network 10.4.4.0 255.255.255.0
BR3(dhcp-config)#default-router 10.4.4.254
BR3(dhcp-config)#dns-server 8.8.8.8
BR3(dhcp-config)#lease infinite
BR3(dhcp-config)#exit
BR3(config)#ip dhcp excluded-address 10.4.4.101 10.4.4.254
```

✳️ BR4

```
!-- 기본 설정
Router>en
Router#conf t
Router(config)#host BR4
BR4(config)#no ip domain-lookup
BR4(config)#line con 0
BR4(config-line)#exec-timeout 0
BR4(config-line)#logging sync

!-- 인터페이스 설정
BR4(config)#int g0/0
BR4(config-if)#ip add 10.5.5.254 255.255.255.0
BR4(config-if)#no sh
BR4(config-if)#int g0/1
BR4(config-if)#ip add 1.1.100.7 255.255.255.0
BR4(config-if)#no sh

!-- OSPF 설정
BR4(config)#router ospf 10
BR4(config-router)#network 1.1.100.7 0.0.0.0 area 0

!-- EIGRP 설정
BR4(config)#router eigrp 10
BR4(config-router)#no auto-summary
BR4(config-router)#network 10.5.5.254 0.0.0.0
BR4(config-router)#network 10.100.1.5 0.0.0.0

!-- mGRE 설정
BR4(config)#int tunnel 0
BR4(config-if)#ip address 10.100.1.5 255.255.255.0
BR4(config-if)#ip nhrp authentication cisco
BR4(config-if)#tunnel source 1.1.100.7
BR4(config-if)#tunnel mode gre multipoint
BR4(config-if)#tunnel key 10

!-- NHRP 설정
BR4(config-if)#ip nhrp network-id 10
BR4(config-if)#ip nhrp nhs 10.100.1.1
BR4(config-if)#ip nhrp map 10.100.1.1 1.1.200.1
BR4(config-if)#ip nhrp map multicast 1.1.200.1
BR4(config-if)#ip nhrp registration timeout 60

!-- IPSec 설정
BR4(config)#crypto isakmp policy 10
BR4(config-isakmp)#authentication pre-share
BR4(config-isakmp)#encr aes
BR4(config-isakmp)#exit
BR4(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0
BR4(config)#crypto ipsec transform-set ts_BR->HQ esp-aes esp-sha-hmac
BR4(cfg-crypto-trans)#mode transport
BR4(cfg-crypto-trans)#crypto ipsec profile pf_HQ_BR_VPN
BR4(ipsec-profile)#set transform-set ts_BR->HQ
BR4(ipsec-profile)#exit
BR4(config)#int tunnel 0
BR4(config-if)#tunnel protection ipsec profile pf_HQ_BR_VPN

!-- DHCP 설정
BR4(config)#ip dhcp pool BR_pool
BR4(dhcp-config)#network 10.5.5.0 255.255.255.0
BR4(dhcp-config)#default-router 10.5.5.254
BR4(dhcp-config)#dns-server 8.8.8.8
BR4(dhcp-config)#lease infinite
BR4(dhcp-config)#exit
BR4(config)#ip dhcp excluded-address 10.5.5.101 10.5.5.254
```

💠 HOST

🖥️ BR1_1 - 4-2

```
VPCS> set pcname pos1_1 - 4-2
pos1_1> ip dhcp -r
```