



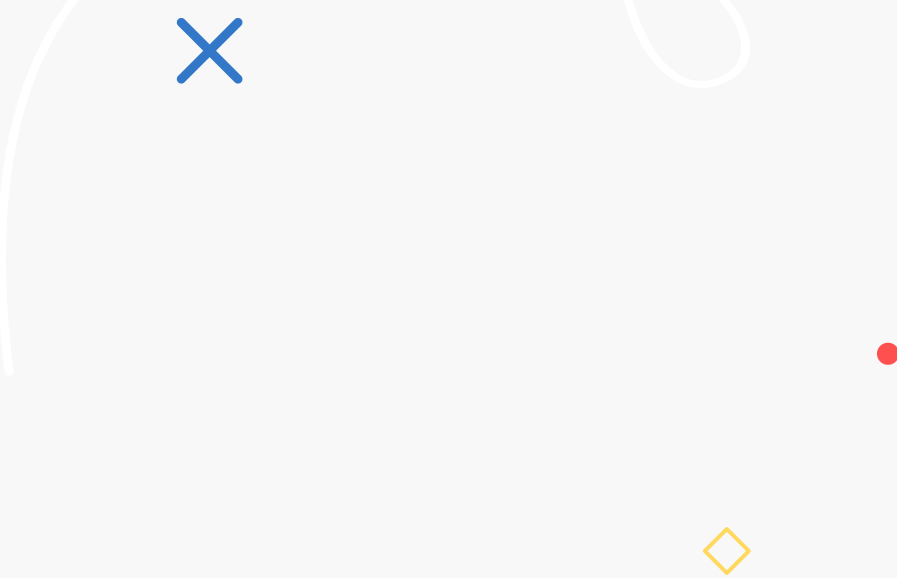
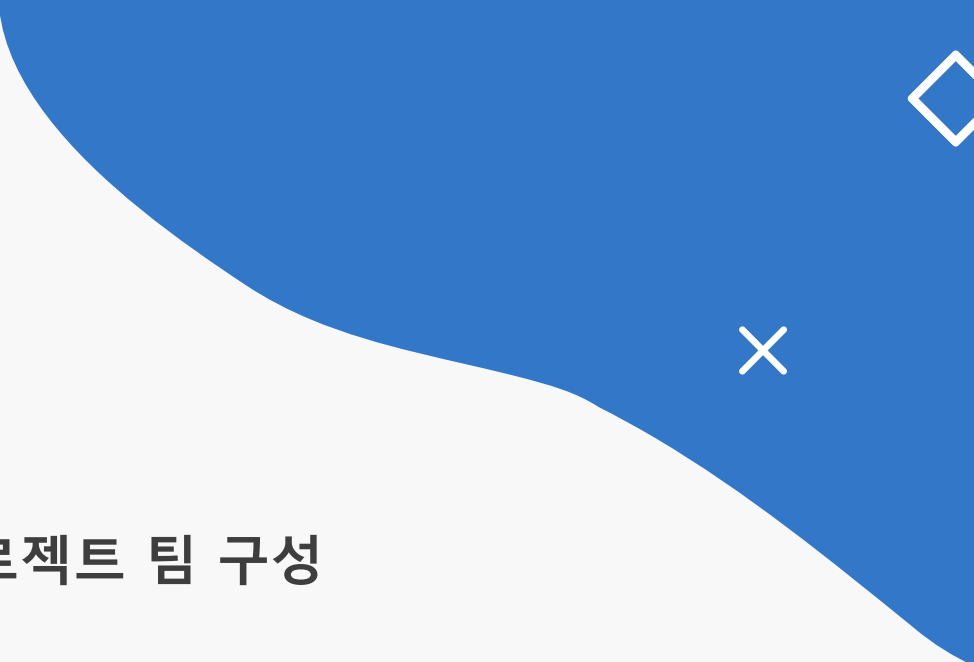
CCTV 본사 보안 인프라 설계 및 구축

1조

권효중, 이효운, 연광흠, 지승헌

목 차



- 01 프로젝트 팀 구성
 - 02 프로젝트 수행 절차
 - 03 프로젝트 개요
 - 04 프로젝트 수행 경과
 - 05 기대효과 및 소감
- 
- 

01 프로젝트 팀 구성

성 명	역할	담당 업무
권효중	Project Manager FireWall	FireWall 구축 및 발표 자료 작성
이효운	Project Leader DMZ	DMZ 구축 및 보고서 작성
연광흠	Project Leader IPS & IDS	IPS 구축 및 보고서 작성
지승헌	Project Leader Proxy	Proxy 구축 및 보고서 작성, 산출물 작성

프로젝트 수행 절차

프로젝트 일정 계획

[illegible]

03 프로젝트 개요

▶ 프로젝트 주제

프로젝트 주제

CCTV 본사 네트워크의 KVM 기반 백본망 및 보안 인프라 설계 및 구축

WHY

CCTV 영상 및 관련 서비스 데이터를 안전하게 보호하고, 내부 네트워크의 보안성을 극대화하며 원활한 트래픽 관리를 통해 고성능 감시 시스템 및 안정적인 서비스 구현

03 프로젝트 개요

▶ 프로젝트 목적

WHAT

원활한 트래픽 관리

고가용성 및 데이터 보안 향상

안정적인 서비스 이용

03 프로젝트 개요

▶ 프로젝트 시나리오

WHERE

Non Blind Site(NBS) 본사 네트워크 망 – IPS/IDS, FireWall, DMZ, Proxy

WHO

본사 내부망에 접근하는 외부 및 내부 사용자, 직원, 클라이언트

HOW

OSPF, NAT, VRRP, FireWall Rules, Static Routing, IPS/IDS Rules, Load Balancing, Transparent Proxy

03 프로젝트 개요

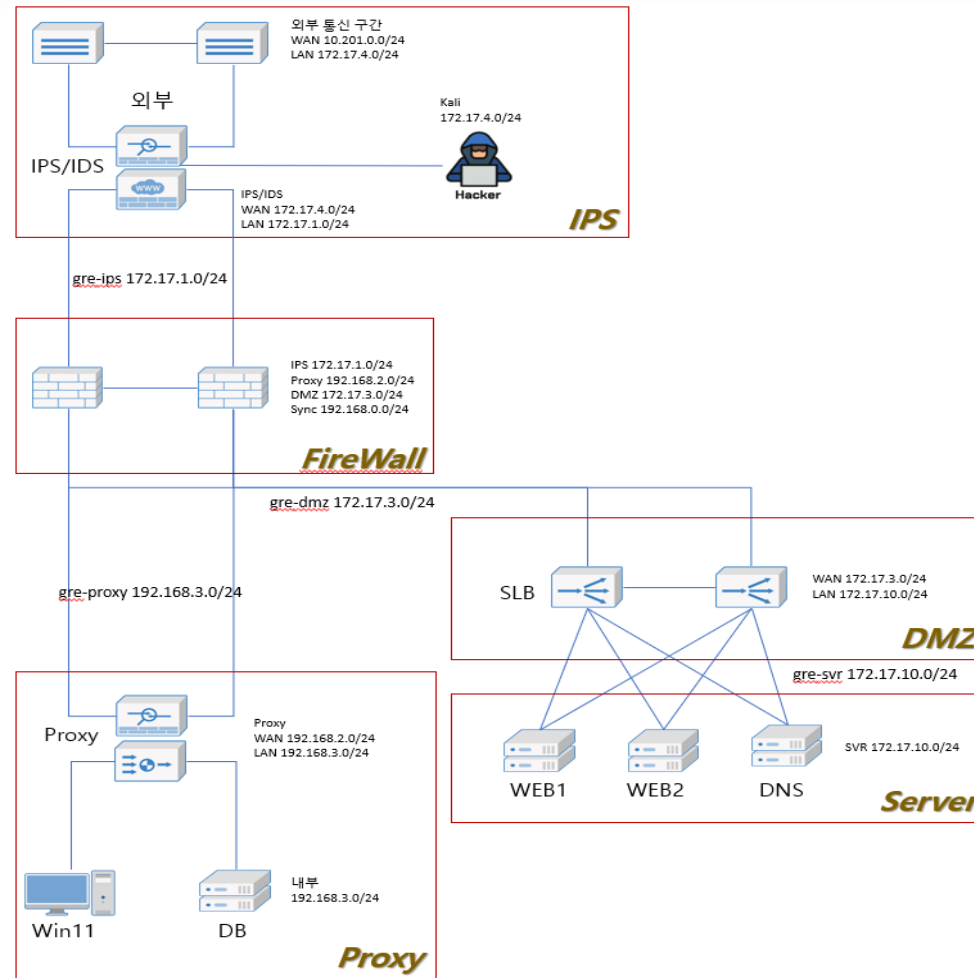
▶ 배경 기술

OS & SW

Alma Linux9, Window11, Kali Linux, OPNsense, Vynos
VMware, KVM, DNS server, WAS, MariaDB, PHP

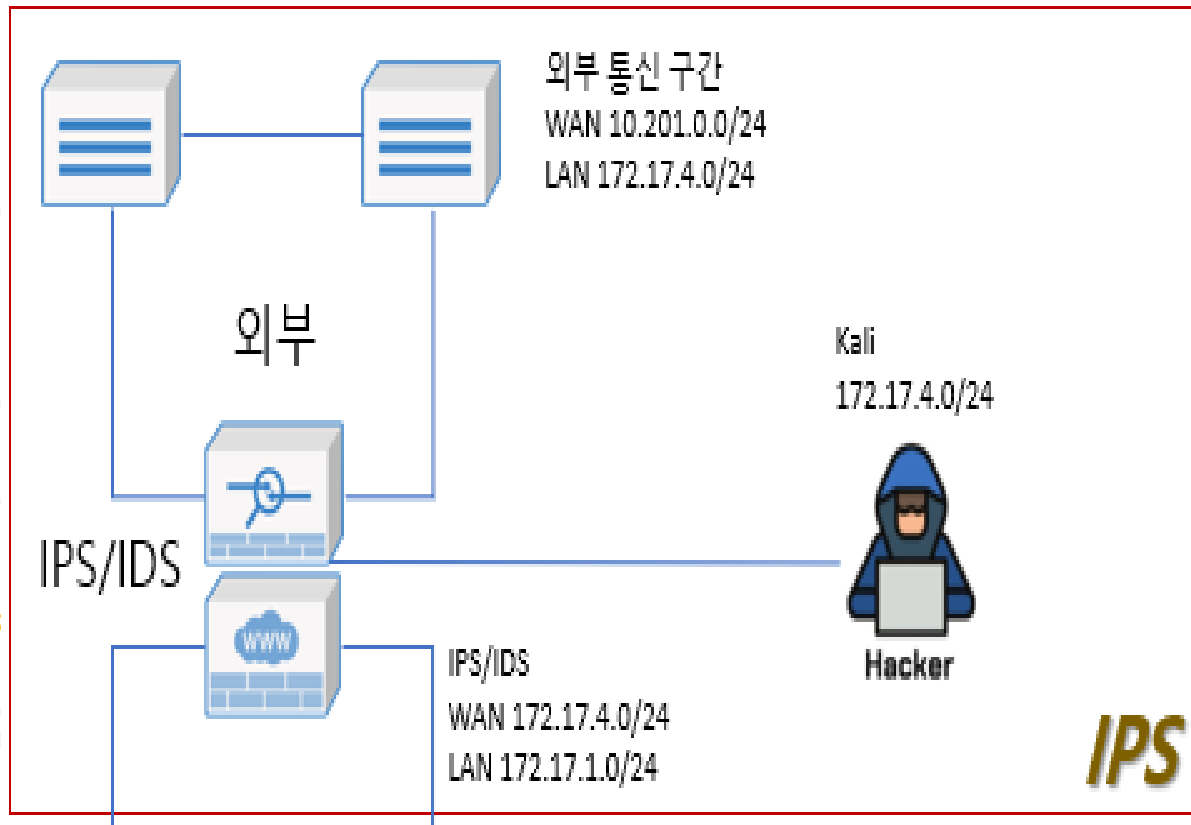
03 프로젝트 개요

▶ 전체 구성도



04 프로젝트 수행경과

▶ 수행경과 - IPS/IDS

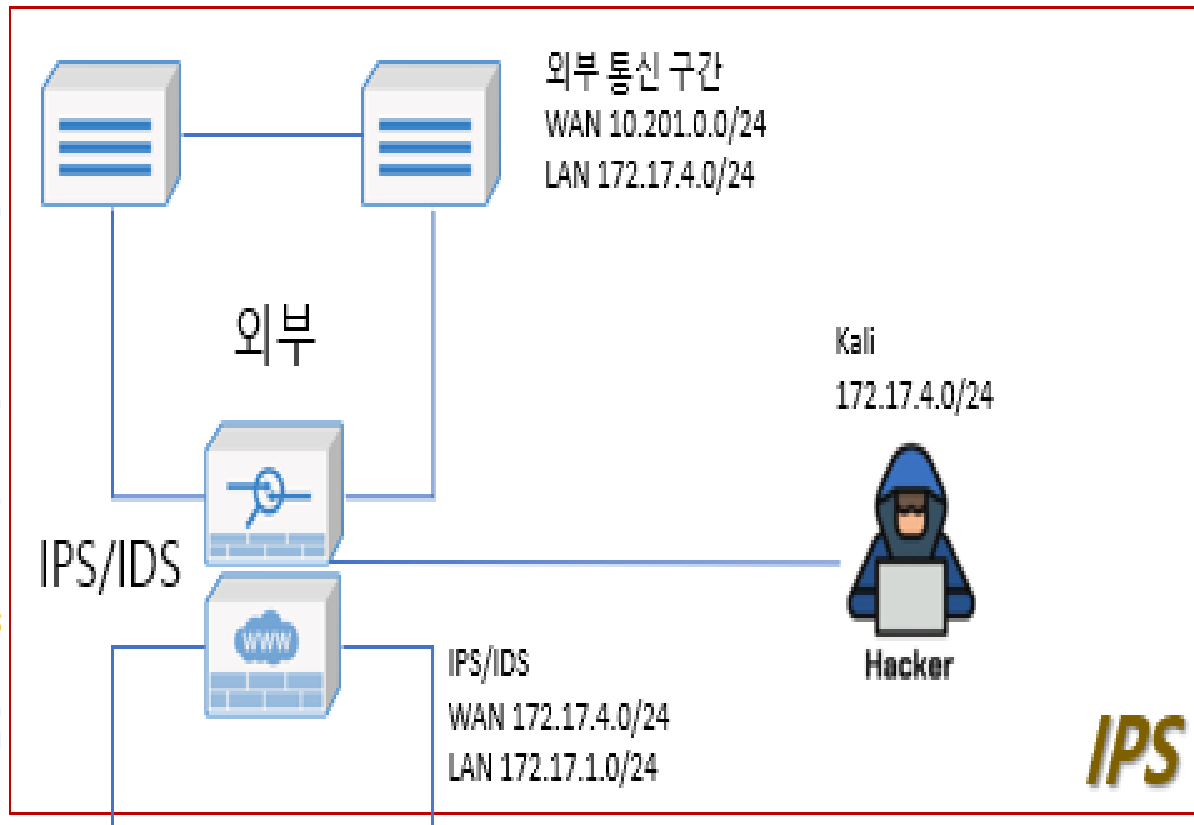


- 외부 통신 구간
- FireWall과 Gre Tunneling
- Vynos 이중화
- IPS/IDS를 통해 침입 방지/탐지
- NAT 설정

04 프로젝트 수행경과

▶ 수행경과 - IPS/IDS

GRE Tunneling 설정

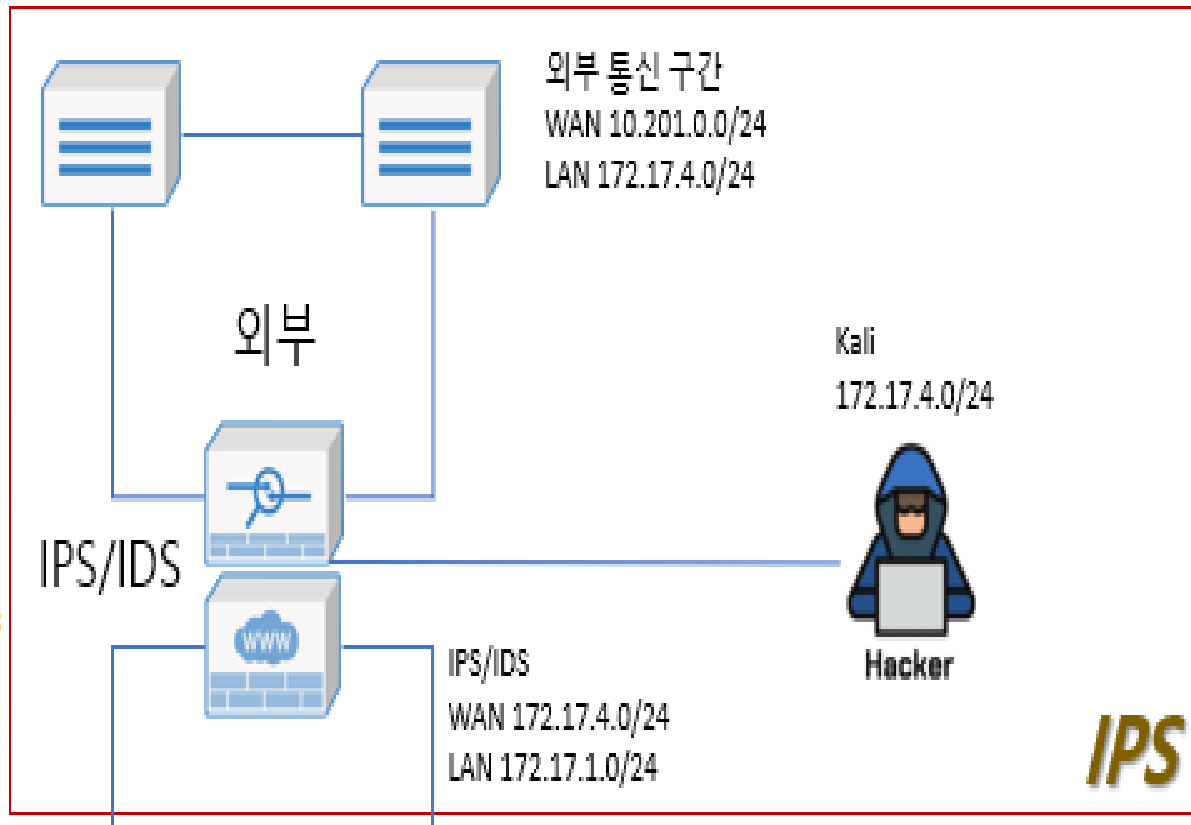


```
[root@kvm nfs]# ovs-vsctl show
e39d77a1-7547-4b41-b500-3bc5d8606348
    Bridge gre-ips
        Port gre1
            Interface gre1
                type: gre
                options: {key="1", remote_ip="10.201.0.2"}
        Port gre-ips
            Interface gre-ips
                type: internal
        Port vnet0
            Interface vnet0
    ovs_version: "3.4.2-39.el9s"
```

04 프로젝트 수행경과

▶ 수행경과 - IPS/IDS

Interface 설정



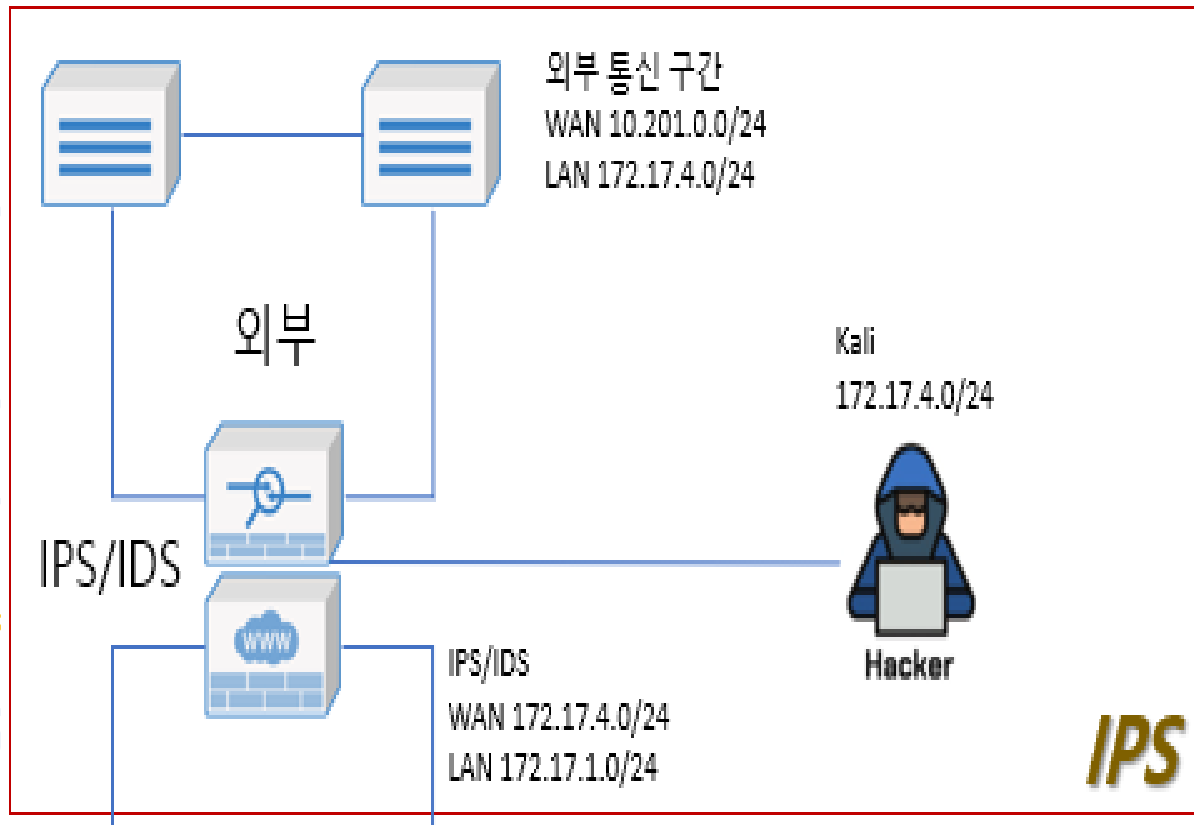
```
vyos@vyos# ru show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface  IP Address      MAC                VRF      MTU  S/L  Description
-----
eth0       172.17.4.11/24   52:54:00:f5:8d:f0  default  1500 u/u
           172.17.4.1/24
eth1       10.201.0.101/8   52:54:00:54:b8:28  default  1500 u/u
           10.201.0.100/8
lo         127.0.0.1/8      00:00:00:00:00:00  default  65536 u/u
           ::1/128
```

```
vyos@vyos# ru show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface  IP Address      MAC                VRF      MTU  S/L  Description
-----
eth0       172.17.4.12/24   52:54:00:b9:b0:35  default  1500 u/u
eth1       10.201.0.102/8   52:54:00:0e:9b:e9  default  1500 u/u
lo         127.0.0.1/8      00:00:00:00:00:00  default  65536 u/u
           ::1/128
```

04 프로젝트 수행경과

▶ 수행경과 - IPS/IDS

VRRP 설정



```
vyos@vyos# ru show vrrp
```

Name	Interface	VRID	State	Priority	Last Transition
1	eth0	1	MASTER	200	23h46m22s
2	eth1	2	MASTER	200	23h46m22s

```
[edit]
```

```
vyos@vyos# ru show vrrp
```

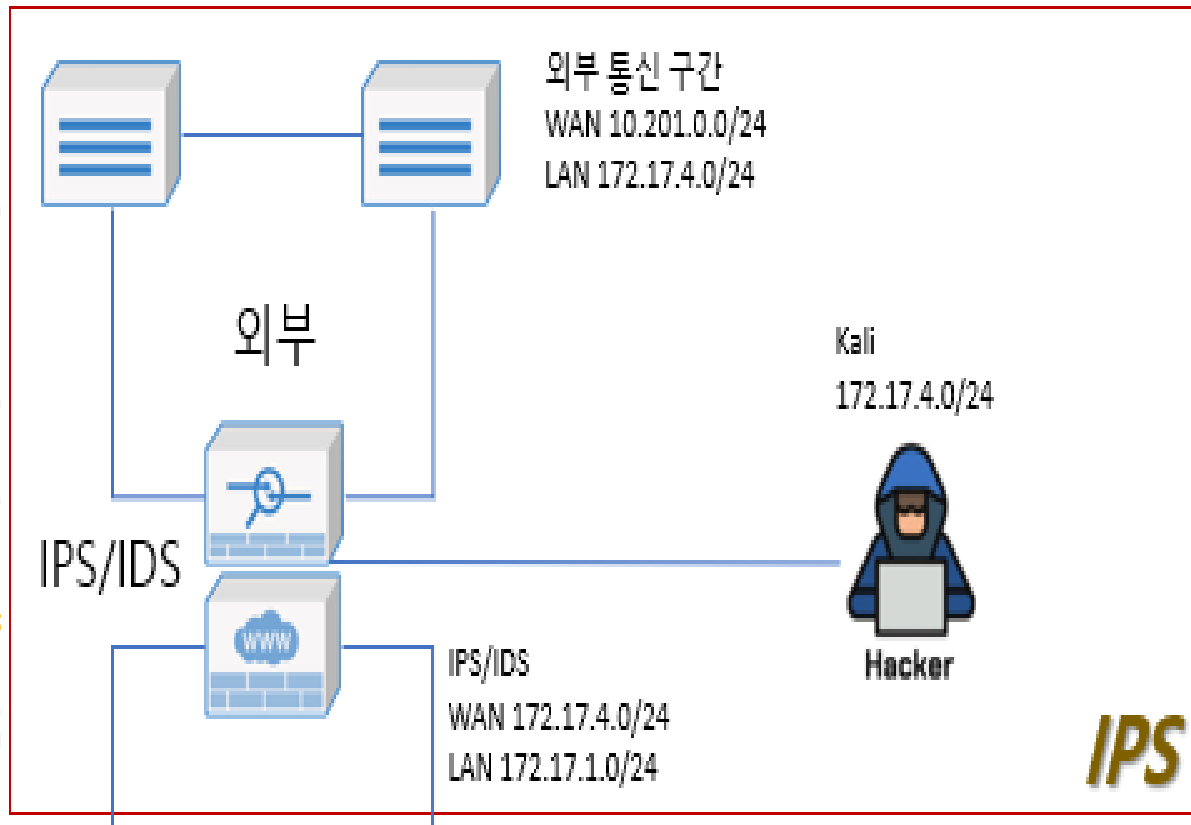
Name	Interface	VRID	State	Priority	Last Transition
1	eth0	1	BACKUP	100	1h14m40s
2	eth1	2	BACKUP	100	1h14m40s

```
[edit]
```

04 프로젝트 수행경과

▶ 수행경과 - IPS/IDS

OSPF 설정

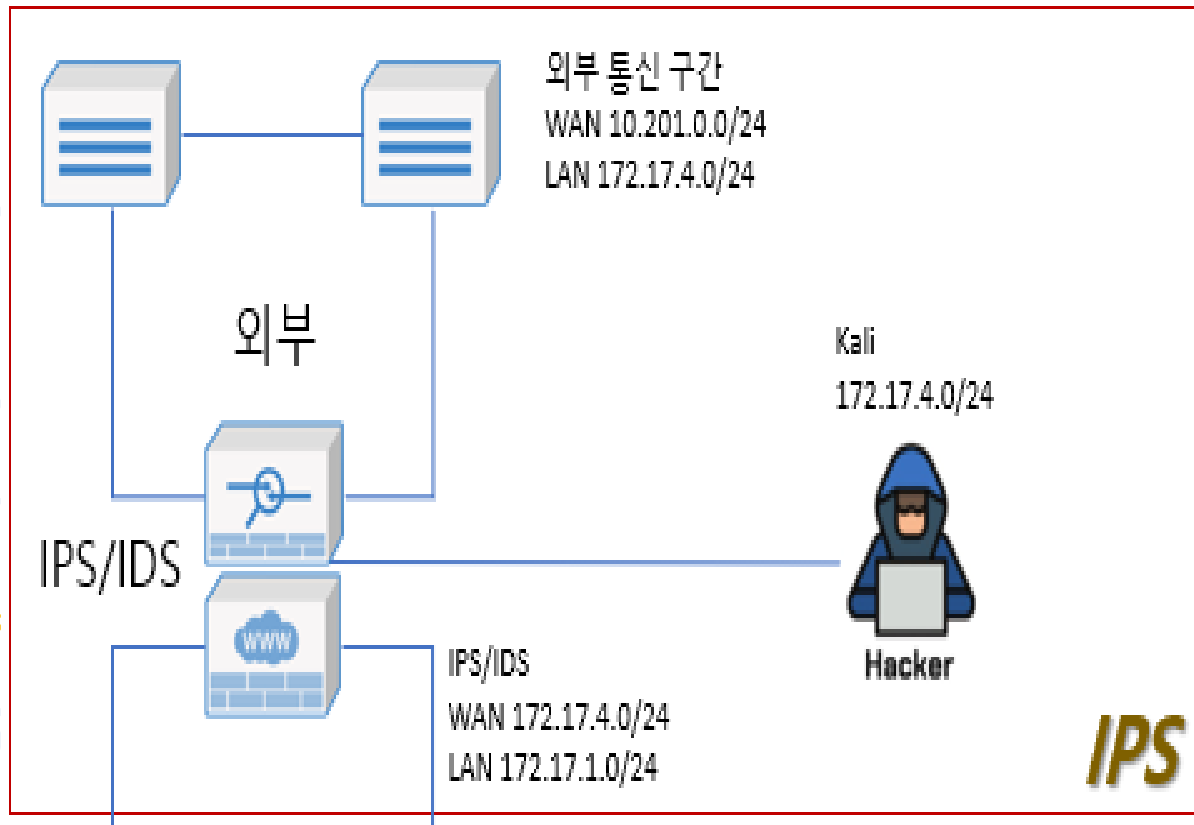


```
protocols {
    ospf {
        area 0.0.0.0 {
        }
        default-information {
            originate {
            }
        }
        interface eth0 {
            area 0.0.0.0
        }
        interface eth1 {
            area 0.0.0.0
        }
    }
    static {
        route 0.0.0.0/0 {
            next-hop 10.0.0.1 {
            }
        }
        route 172.17.0.0/16 {
        }
    }
}
```

04 프로젝트 수행경과

▶ 수행경과 - IPS/IDS

NAT 설정

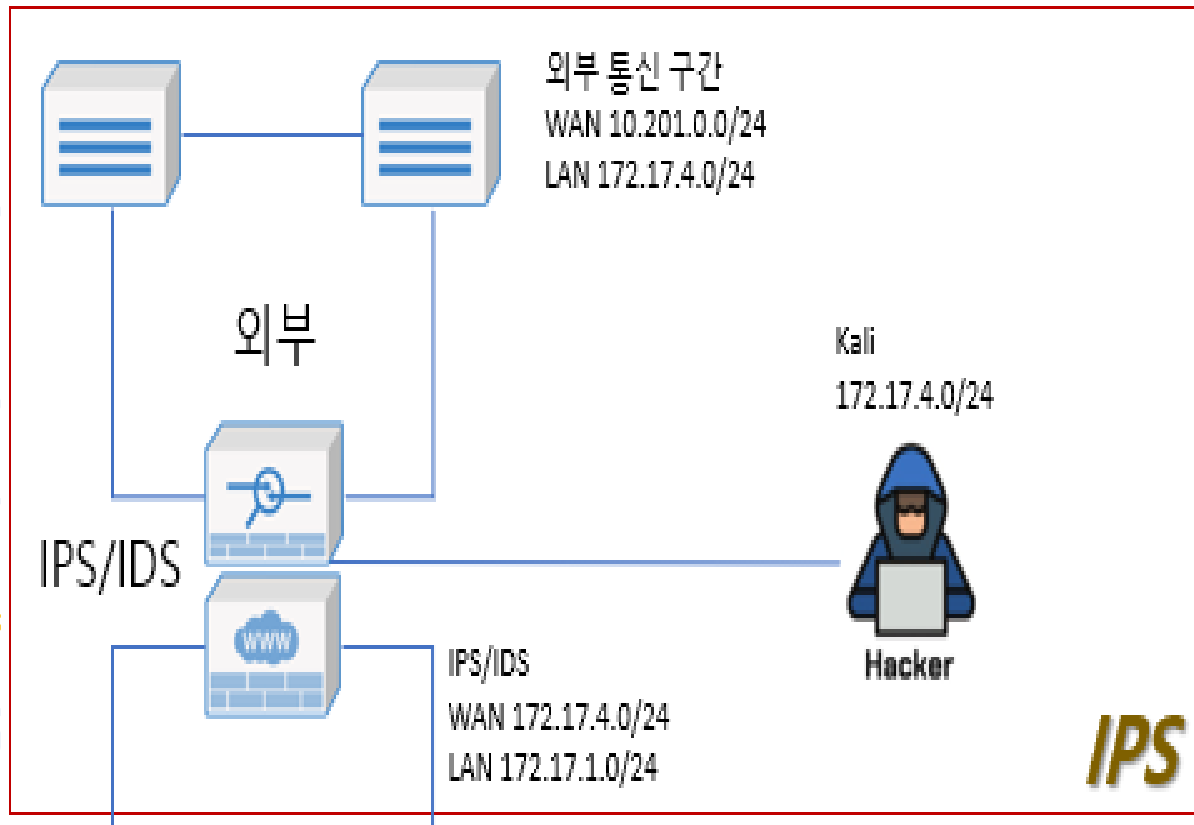


```
nat {  
  destination {  
    rule 30 {  
      description "Forward HTTP to 172.17.10.101"  
      destination {  
        address 10.201.0.100  
        port 80  
      }  
      inbound-interface {  
        name eth1  
      }  
      protocol tcp  
      translation {  
        address 172.17.10.10  
        port 80  
      }  
    }  
  }  
  source {  
    rule 10 {  
      outbound-interface {  
        name eth1  
      }  
      source {  
        address 172.17.0.0/16  
      }  
      translation {  
        address masquerade  
      }  
    }  
  }  
}
```

04 프로젝트 수행경과

▶ 수행경과 - IPS/IDS

Routing Table 화면

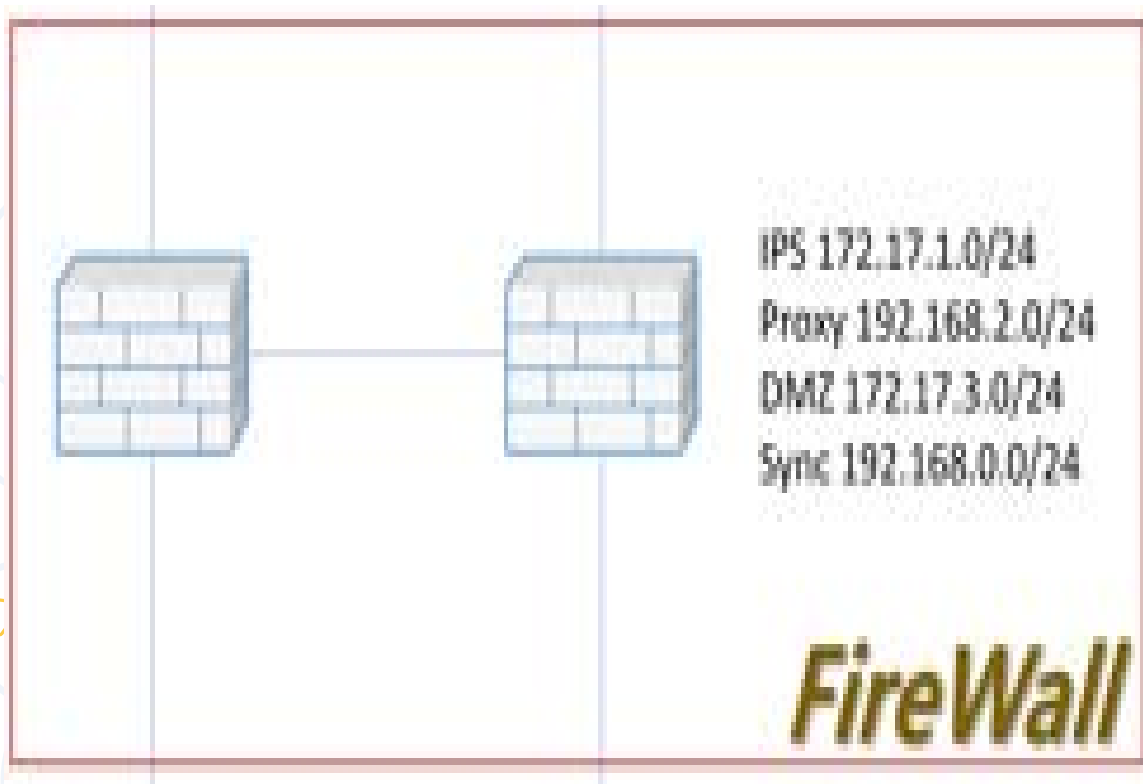


```
vyos@vyos# ru show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O   0.0.0.0/0 [110/10] via 10.0.0.1, eth1, weight 1, 23:46:18
S>* 0.0.0.0/0 [1/0] via 10.0.0.1, eth1, weight 1, 23:46:48
O   10.0.0.0/8 [110/1] is directly connected, eth1, weight 1, 23:46:24
C>* 10.0.0.0/8 is directly connected, eth1, 23:46:50
O>* 172.17.1.0/24 [110/2] via 10.203.15.2, eth1, weight 1, 23:46:24
    * via 10.203.15.3, eth1, weight 1, 23:46:24
O>* 172.17.2.0/24 [110/12] via 10.203.15.2, eth1, weight 1, 05:14:24
    * via 10.203.15.3, eth1, weight 1, 05:14:24
O>* 172.17.3.0/24 [110/21] via 172.17.4.100, eth0, weight 1, 23:45:57
O   172.17.4.0/24 [110/1] is directly connected, eth0, weight 1, 23:46:47
C>* 172.17.4.0/24 is directly connected, eth0, 23:46:50
O>* 172.17.10.0/24 [110/22] via 172.17.4.100, eth0, weight 1, 23:45:57
O>* 172.17.100.0/24 [110/22] via 10.203.15.2, eth1, weight 1, 05:14:24
    * via 10.203.15.3, eth1, weight 1, 05:14:24
O>* 172.17.101.0/24 [110/23] via 10.203.15.2, eth1, weight 1, 00:01:21
    * via 10.203.15.3, eth1, weight 1, 00:01:21
O>* 172.17.200.0/24 [110/22] via 10.203.15.2, eth1, weight 1, 05:14:24
    * via 10.203.15.3, eth1, weight 1, 05:14:24
O>* 192.168.0.0/24 [110/21] via 172.17.4.100, eth0, weight 1, 23:45:57
O>* 192.168.50.0/24 [110/20] via 10.203.15.2, eth1, weight 1, 05:14:23
    * via 10.203.15.3, eth1, weight 1, 05:14:23
O>* 192.168.51.0/24 [110/32] via 10.203.15.2, eth1, weight 1, 05:14:24
    * via 10.203.15.3, eth1, weight 1, 05:14:24
[edit]
```


04 프로젝트 수행경과

▶ 수행경과 - FireWall

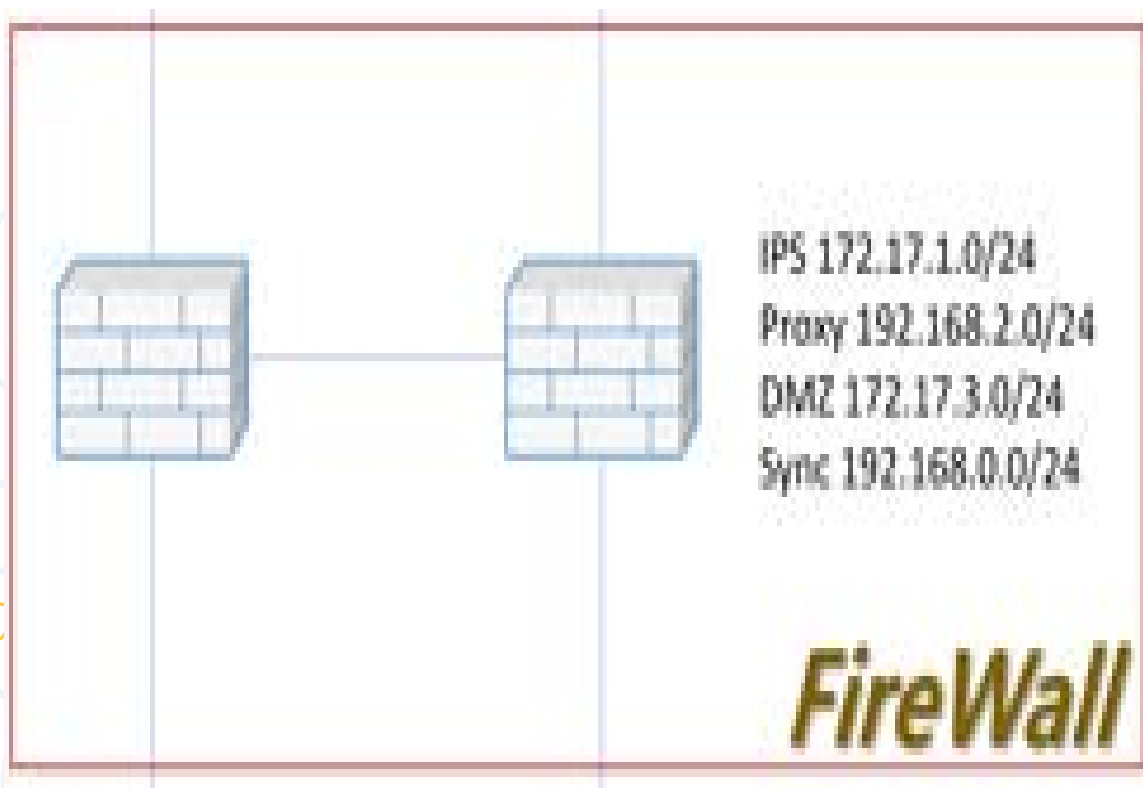


- 외부 내부 연결 구간
- IPS/IDS, DMZ, Proxy와 GRE Tunneling
- NAT OutBound 설정
- OPNsense 이중화
- FireWall Rules 및 Static Routing 설정
- IPS/IDS, DMZ 와 OSPF 설정
- SYNC 설정

04 프로젝트 수행경과

▶ 수행경과 - FireWall

GRE Tunneling 설정

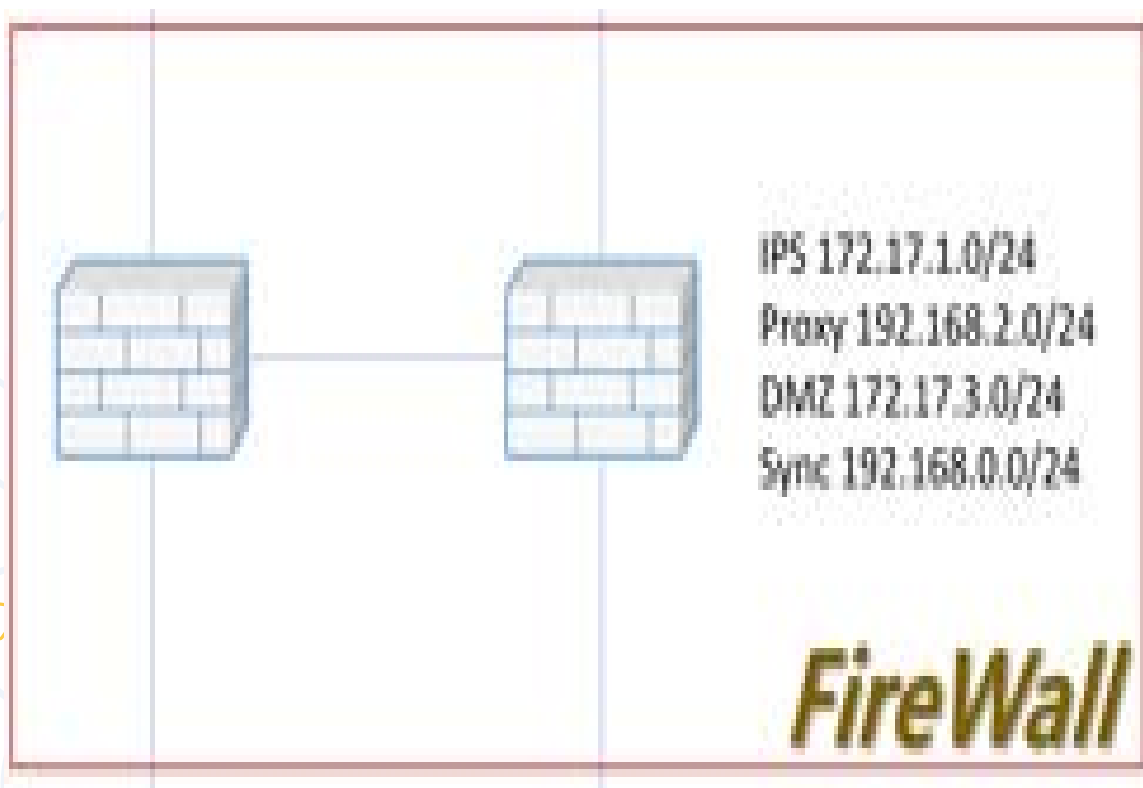


```
[root@localhost ~]# ovs-vsctl show
bb0065a1-5606-477d-86cd-967eb292a656
  Bridge gre-ips
    Port vnet5
      Interface vnet5
    Port vnet1
      Interface vnet1
    Port gre-ips
      Interface gre-ips
        type: internal
    Port gre1
      Interface gre1
        type: gre
        options: {key="1", remote_ip="10.201.0.16"}
  Bridge gre-dmz
    Port vnet6
      Interface vnet6
    Port gre3
      Interface gre3
        type: gre
        options: {key="3", remote_ip="10.201.0.10"}
    Port gre-dmz
      Interface gre-dmz
        type: internal
    Port vnet2
      Interface vnet2
  Bridge gre-proxy
    Port gre2
      Interface gre2
        type: gre
        options: {key="2", remote_ip="10.201.0.3"}
    Port gre-proxy
      Interface gre-proxy
        type: internal
    Port vnet0
      Interface vnet0
    Port vnet4
      Interface vnet4
  ovs_version: "3.4.2-39.el9s"
```

04 프로젝트 수행경과

▶ 수행경과 - FireWall

OPNsense VIP 설정



Interfaces: Virtual IPs: Status

Addresses pfSync nodes

Q Search

CARP

7

Interface	VHID	Address	Status
<input type="checkbox"/> LAN	1 (freq. 1/0)	192.168.2.10	▶ MASTER
<input type="checkbox"/> WAN	2 (freq. 1/0)	172.17.1.10	▶ MASTER
<input type="checkbox"/> OPT	3 (freq. 1/0)	172.17.3.10	▶ MASTER

Showing 1 to 3 of 3 entries

Interfaces: Virtual IPs: Status

Addresses pfSync nodes

Q Search

CARP

7

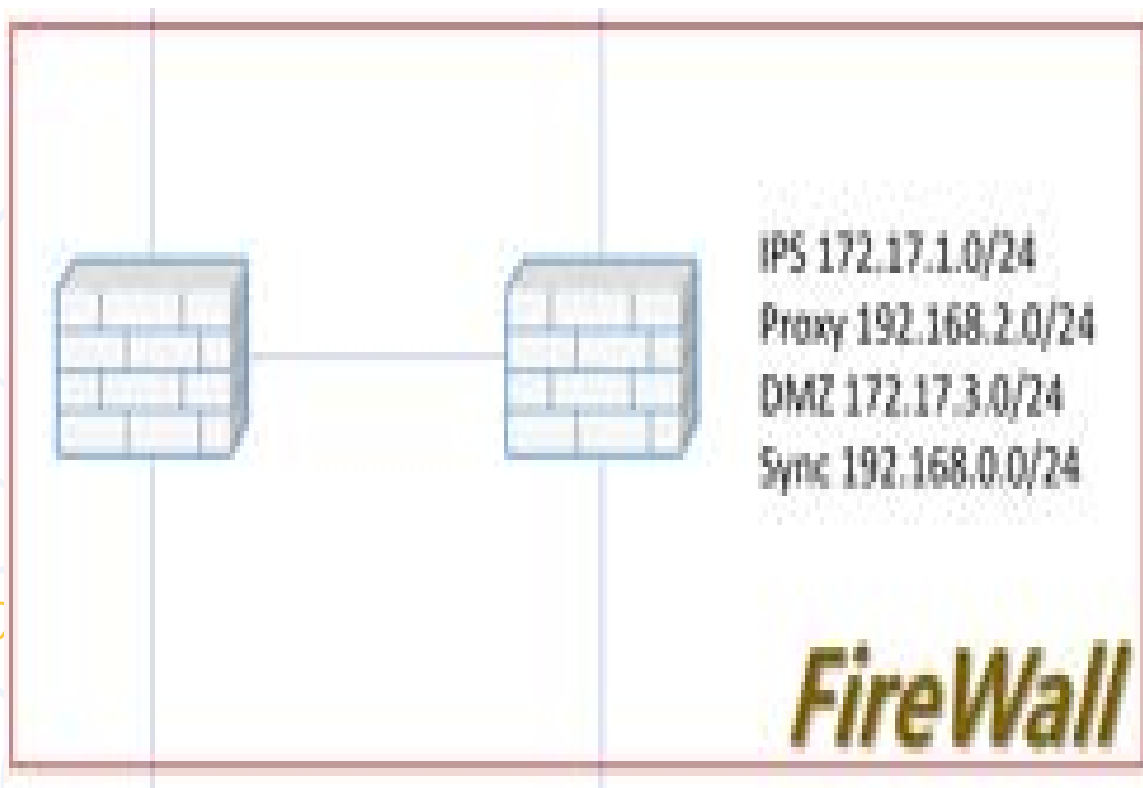
Interface	VHID	Address	Status
<input type="checkbox"/> LAN	1 (freq. 3/0)	192.168.2.10	▶ BACKUP
<input type="checkbox"/> WAN	2 (freq. 3/0)	172.17.1.10	▶ BACKUP
<input type="checkbox"/> OPT	3 (freq. 3/0)	172.17.3.10	▶ BACKUP

Showing 1 to 3 of 3 entries

04 프로젝트 수행경과

▶ 수행경과 - FireWall

SYNC High Availability 설정



System: High Availability: Status

Backup firewall versions

Firmware	Base	Kernel
24.7	24.7	24.7

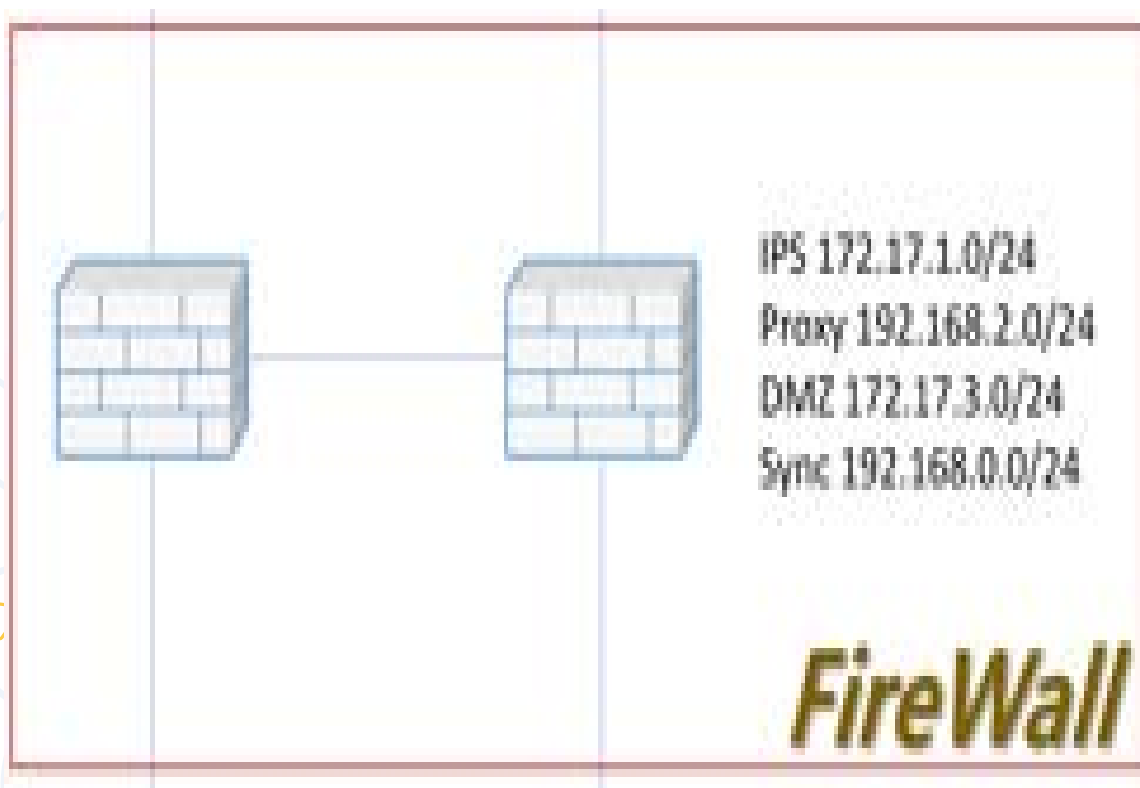
Backup services

Service	Description	Status
Synchronize	Synchronize config to backup	
Templates	Generate configuration templates	
configd	System Configuration Daemon	
cron	Cron	
frr	FRRouting Daemon	
login	Users and Groups	
ntpd	Network Time Daemon	
pf	Packet Filter	
routing	System routing	
sysctl	System tunables	
syslog-ng	Syslog-ng Daemon	
unbound	Unbound DNS	
wehavi	Wehavi	

04 프로젝트 수행경과

▶ 수행경과 - FireWall

OSPF 설정



Routing: Diagnostics: OSPF

Overview Routing Table Database Neighbors Interfaces

Type	Network	Cost	Area	Via	Via Interface	Via Interface name
N	10.0.0.0/8	21	0.0.0.0	172.17.1.100	vtnet2	WAN
N	172.17.1.0/24	10	0.0.0.0	Directly Attached	vtnet2	WAN
N	172.17.2.0/24	32	0.0.0.0	172.17.1.100	vtnet2	WAN
N	172.17.3.0/24	10	0.0.0.0	Directly Attached	vtnet3	OPT
N	172.17.4.0/24	20	0.0.0.0	172.17.1.100	vtnet2	WAN
N	172.17.10.0/24	11	0.0.0.0	172.17.3.101	vtnet3	OPT
N	172.17.10.0/24	11	0.0.0.0	172.17.3.102	vtnet3	OPT

Routing: Diagnostics: OSPF

Overview Routing Table Database Neighbors Interfaces

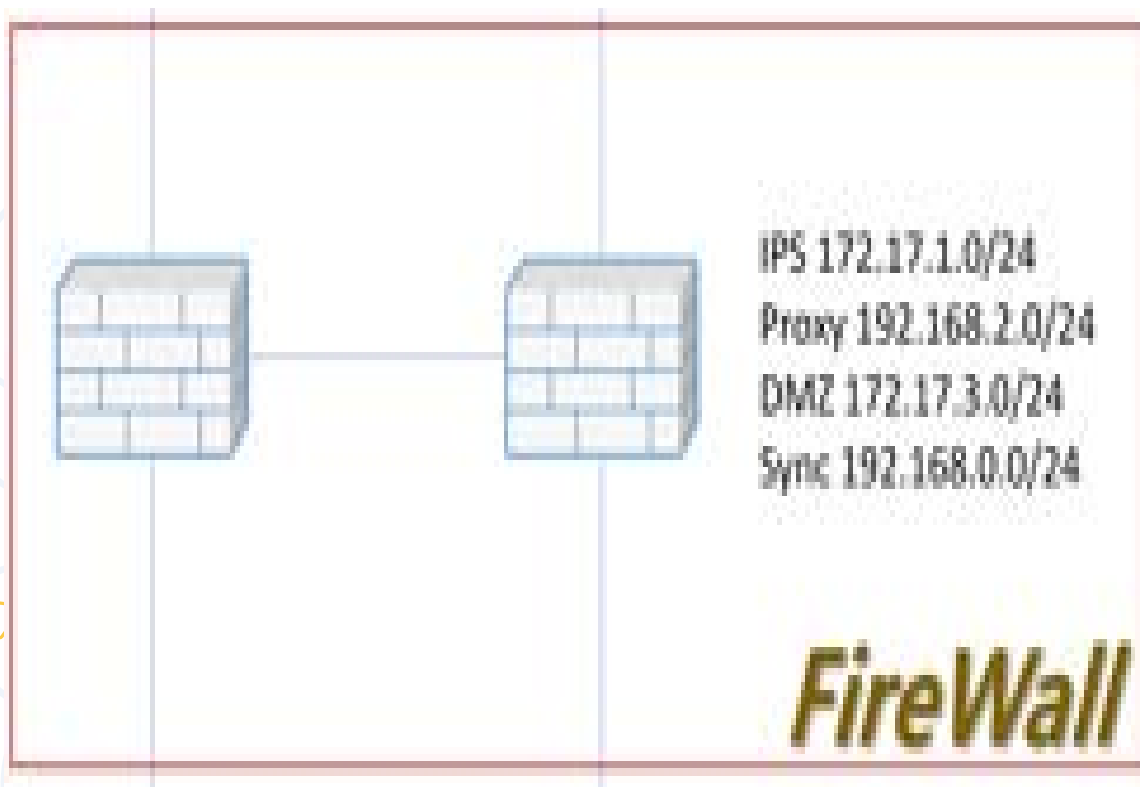
Neighbor ID	Priority	State	Dead Time [ms]	Address	Interface	Retransmit Counter	Request Counter	DB Summary Co...
172.17.4.100	1	Full/DR	36644	172.17.1.100	vtnet2:172.17.1.11	0	0	0
172.17.10.12	1	Full/DR	32421	172.17.3.102	vtnet3:172.17.3.11	0	0	0
172.17.10.11	1	Full/DROther	37954	172.17.3.101	vtnet3:172.17.3.11	0	0	0

Showing 1 to 3 of 3 entries

04 프로젝트 수행경과

▶ 수행경과 - FireWall

NAT Outbound 설정



Firewall: NAT: Outbound

Mode

- ☐ Automatic outbound NAT rule generation
(no manual rules can be used)
- ☒ Manual outbound NAT rule generation
(no automatic rules are being generated)
- ☐ Hybrid outbound NAT rule generation
(automatically generated rules are applied after manual rules)
- ☐ Disable outbound NAT rule generation
(outbound NAT is disabled)

Save

Manual rules

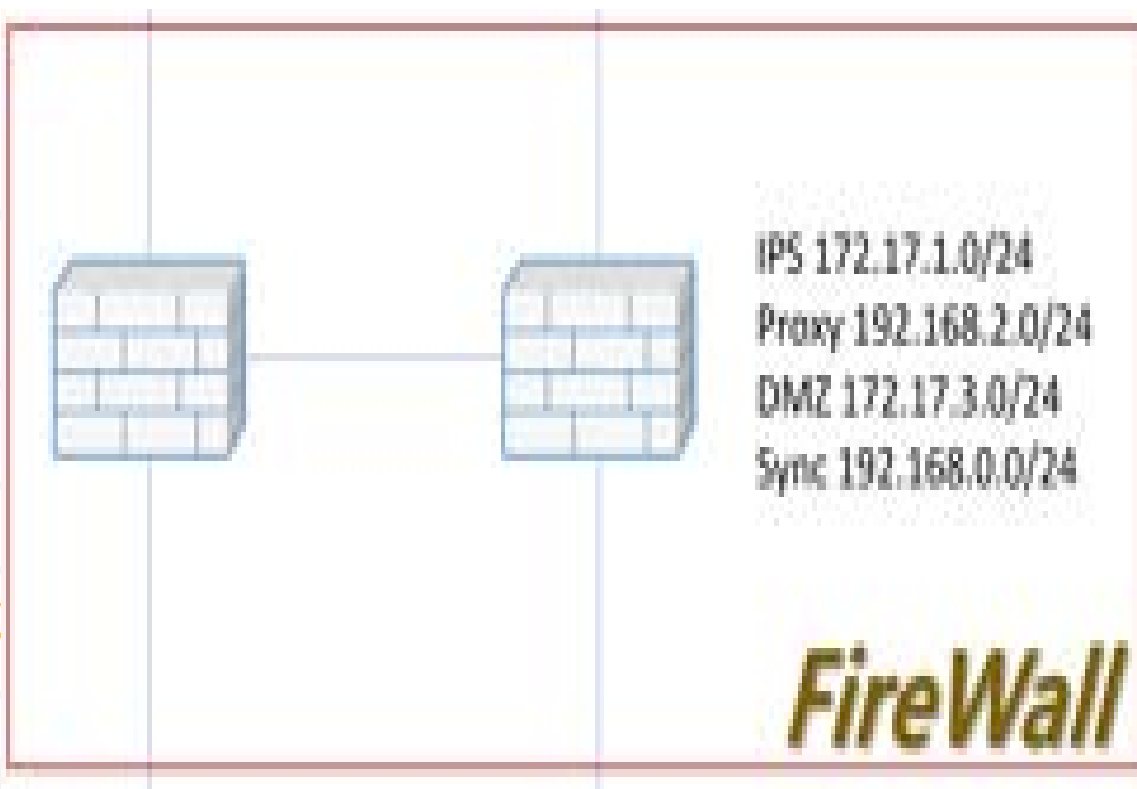
Select category

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	WAN	192.168.0.0/16	*	*	*	172.17.1.10	*	NO		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

04 프로젝트 수행경과

▶ 수행경과 - FireWall

FireWall Rules 설정



Firewall: Rules: LAN

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
Automatically generated rules									
<input type="checkbox"/>	IPv4 TCP	LAN net	*	172.17.10.0/24	80 (HTTP)	*	*		
<input type="checkbox"/>	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	*		
<input type="checkbox"/>	IPv4 UDP	LAN net	*	*	53 (DNS)	*	*		
<input type="checkbox"/>	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	*		

Firewall: Rules: OPT

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
Automatically generated rules									
<input type="checkbox"/>	IPv4 TCP	*	*	*	80 (HTTP)	*	*		
<input type="checkbox"/>	IPv4 TCP	*	*	*	443 (HTTPS)	*	*		
<input type="checkbox"/>	IPv4 UDP	*	*	*	53 (DNS)	*	*		
<input type="checkbox"/>	IPv4 ICMP	172.17.10.0/24	*	192.168.3.0/24	*	*	*		
<input type="checkbox"/>	IPv4 TCP	172.17.10.0/24	*	192.168.3.0/24	22 (SSH)	*	*		

Firewall: Rules: WAN

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
Automatically generated rules									
<input type="checkbox"/>	IPv4 TCP	*	*	172.17.10.0/24	80 (HTTP)	*	*		
<input type="checkbox"/>	IPv4 UDP	*	*	172.17.10.0/24	53 (DNS)	*	*		
<input type="checkbox"/>	IPv4 TCP	*	*	172.17.10.0/24	443 (HTTPS)	*	*		
<input type="checkbox"/>	IPv4 *	WAN net	*	WAN net	*	*	*		

☐ pass
☐ pass (disabled)

☒ block
☒ block (disabled)

☒ reject
☒ reject (disabled)

☒ log
☒ log (disabled)

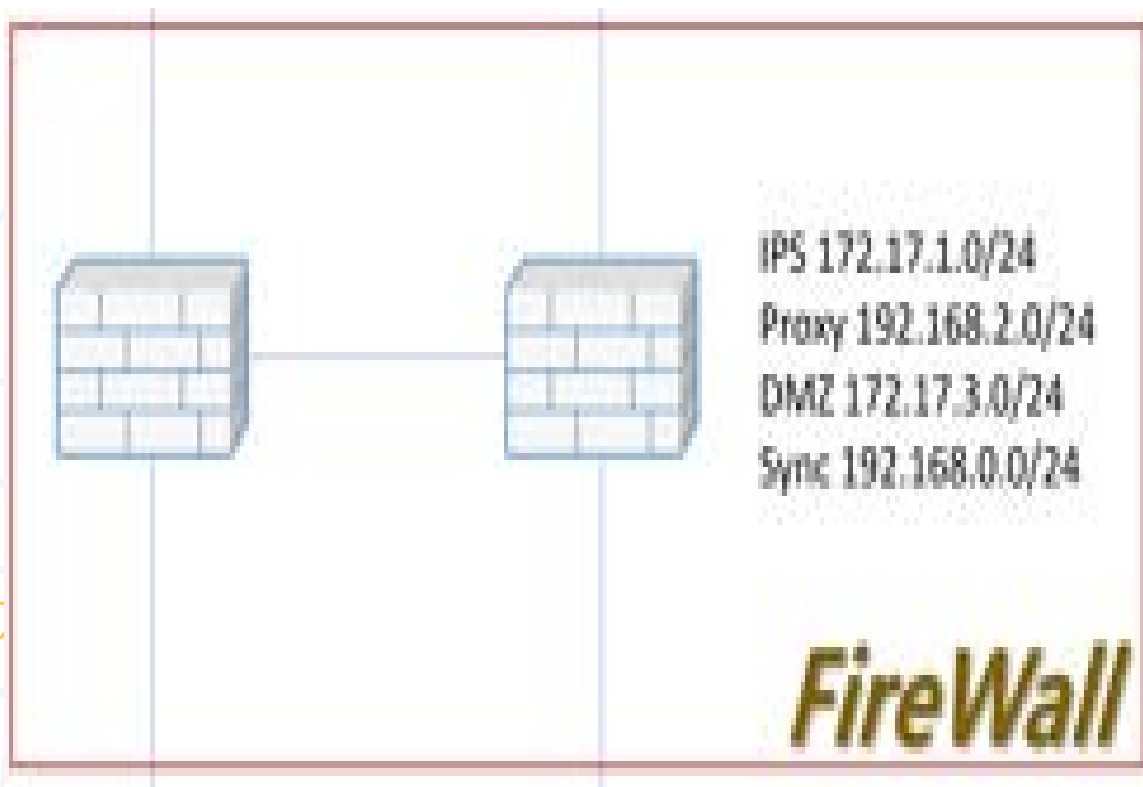
☒ in
☒ out

☒ first match
☒ last match

04 프로젝트 수행경과

▶ 수행경과 - FireWall

Static Routing 설정



Routing: STATIC

General Routes

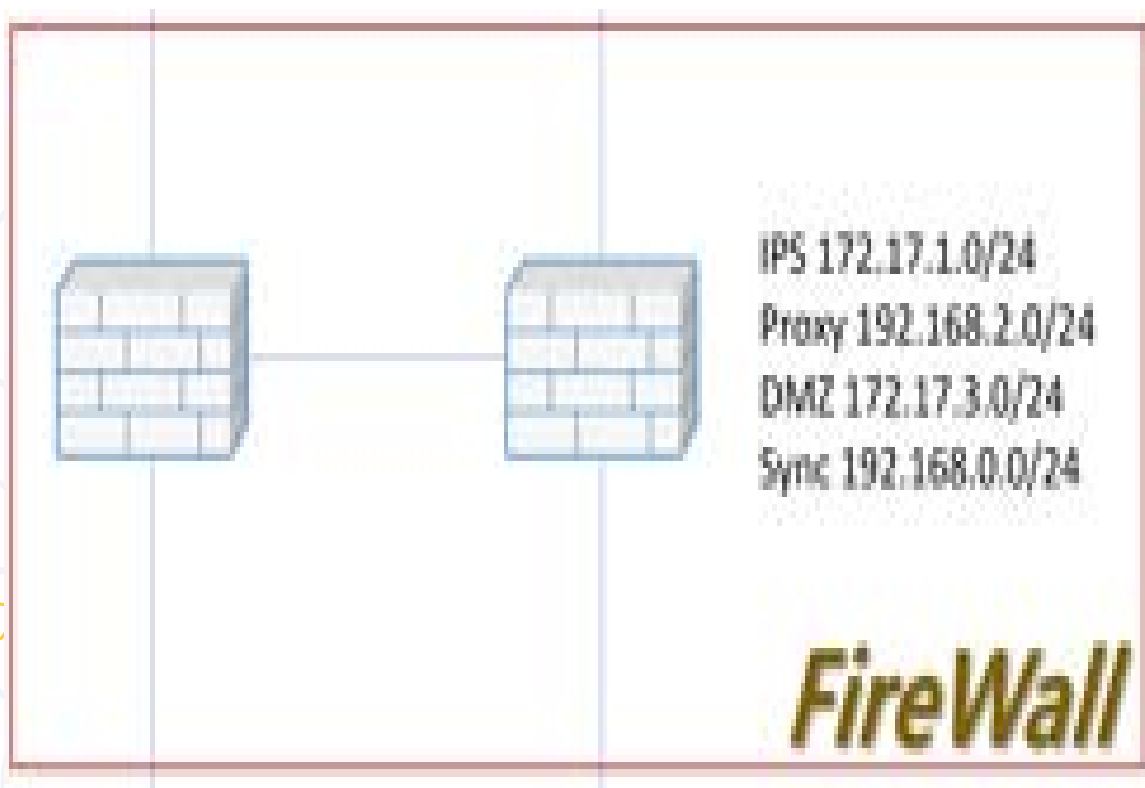
Search

Enabled	Network	Gateway	Interface	Commands
<input type="checkbox"/>	Enabled			
<input checked="" type="checkbox"/>	192.168.3.0/24	192.168.2.101	LAN	

04 프로젝트 수행경과

▶ 수행경과 - FireWall

Routing Table 화면



Routing: Diagnostics: General

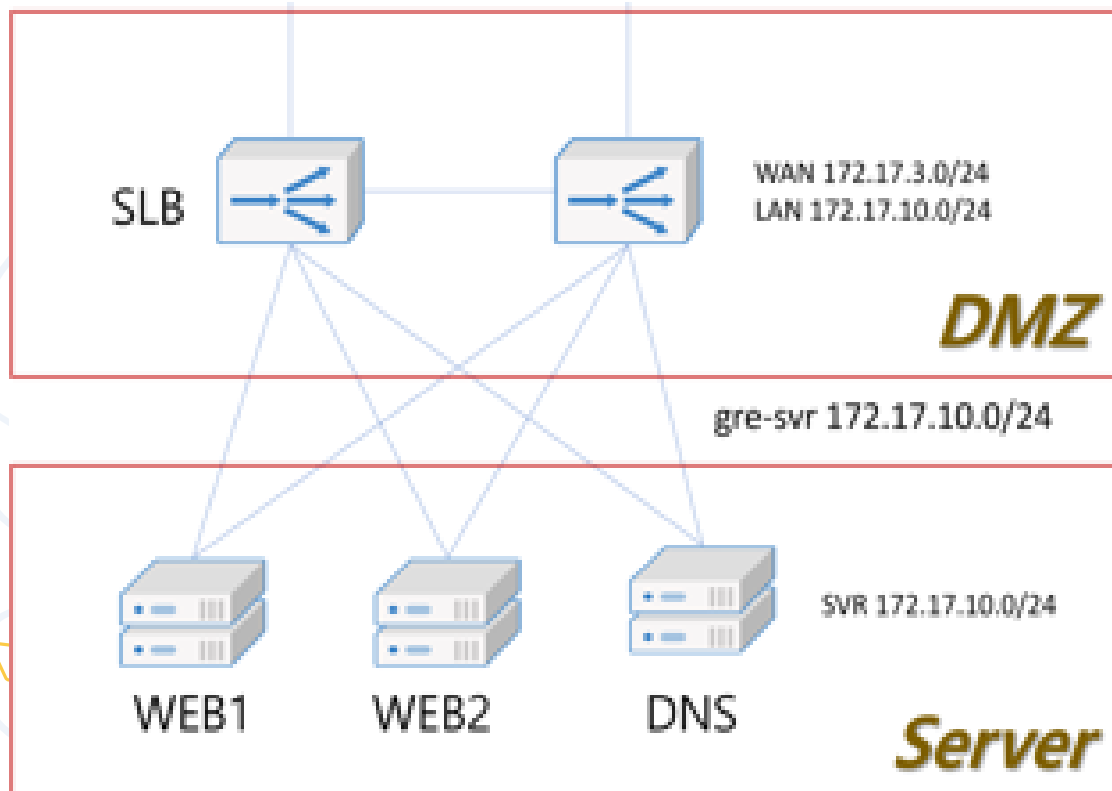
IPv4 Routes IPv6 Routes Running Configuration

Q Search 7 ▾

Code	Network	Administrative Dista...	Metric	Interface	Interface name	Via	Time
O>*	0.0.0.0/0	110	10	vtnet2	WAN	172.17.1.100	00:56:38
O>*	10.0.0.0/8	110	21	vtnet2	WAN	172.17.1.100	00:56:38
O	172.17.1.0/24	110	10	vtnet2	WAN	Directly Attached	00:56:49
C>*	172.17.1.0/24	0	1	vtnet2	WAN	Directly Attached	00:56:49
O>*	172.17.2.0/24	110	32	vtnet2	WAN	172.17.1.100	00:56:38
O	172.17.3.0/24	110	10	vtnet3	OPT	Directly Attached	00:30:41
C>*	172.17.3.0/24	0	1	vtnet3	OPT	Directly Attached	00:56:49
Showing 1 to 7 of 17 entries							
O>*	172.17.4.0/24	110	20	vtnet2	WAN	172.17.1.100	00:57:36
O>*	172.17.10.0/24	110	11	vtnet3	OPT	172.17.3.101	00:30:52
O>*	172.17.10.0/24	110	11	vtnet3	OPT	172.17.3.102	00:30:52
C>*	192.168.0.0/24	0	1	vtnet0	SYNC	Directly Attached	00:58:21
C>*	192.168.2.0/24	0	1	vtnet1	LAN	Directly Attached	00:58:21
S>*	192.168.3.0/24	1	0	vtnet1	LAN	192.168.2.101	00:59:04

04 프로젝트 수행경과

▶ 수행경과 - DMZ

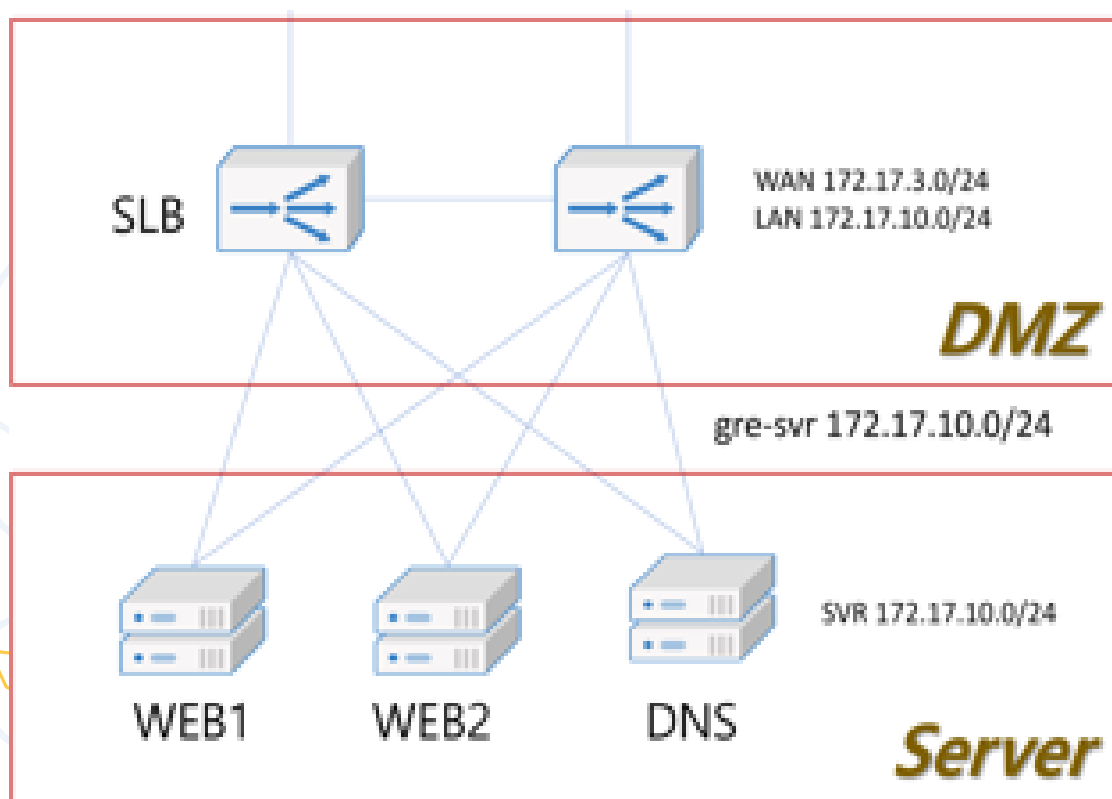


- ServerLoadBalancing(SLB) 설정
- WEB, DNS 서버
- Vynos 이중화
- FireWall, Server, SLB GRE Tunneling
- FireWall 과 OSPF 설정

04 프로젝트 수행경과

▶ 수행경과 - DMZ

GRE Tunneling 설정(SLB 구간)

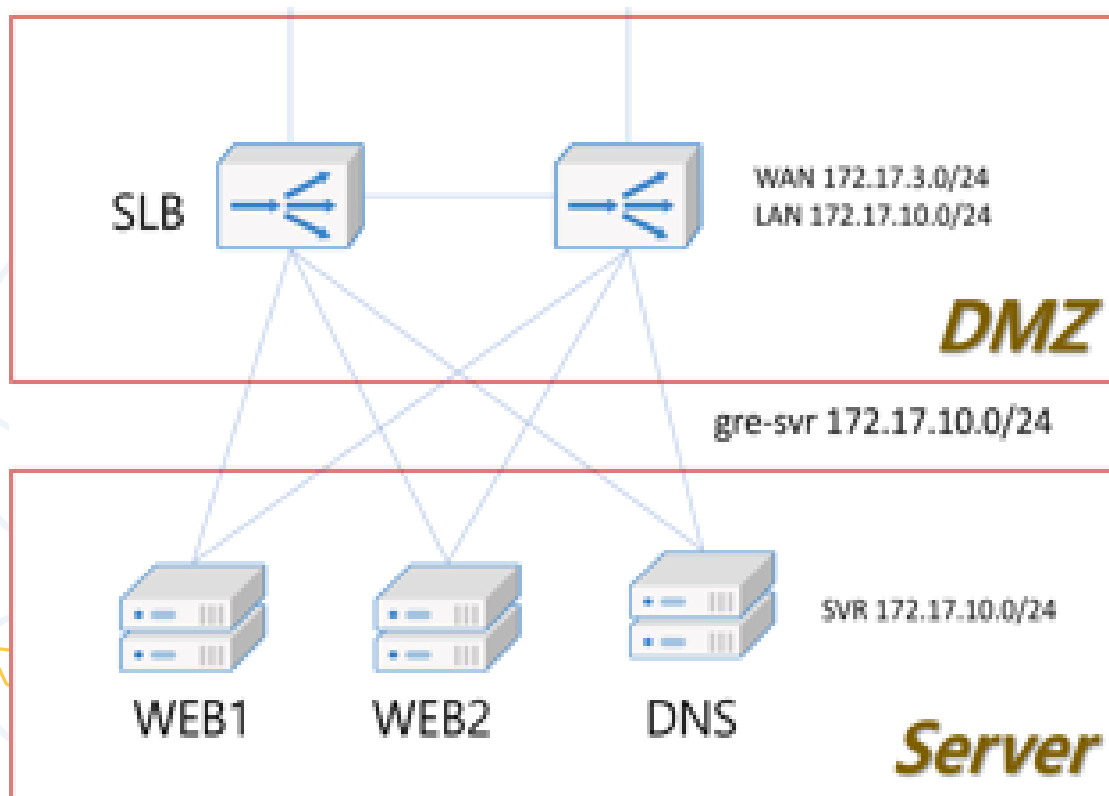


```
[root@localhost ~]# ovs-vsctl show
3de896fd-0fdd-4a1e-a030-a09f9ad9ae9f
    Bridge gre-dmz
        Port vnet0
            Interface vnet0
        Port gre3
            Interface gre3
                type: gre
                options: {key="3", remote_ip="10.201.0.2"}
        Port vnet2
            Interface vnet2
        Port gre-dmz
            Interface gre-dmz
                type: internal
    Bridge gre-svr
        Port gre4
            Interface gre4
                type: gre
                options: {key="4", remote_ip="10.201.0.11"}
        Port vnet1
            Interface vnet1
        Port gre-svr
            Interface gre-svr
                type: internal
        Port vnet3
            Interface vnet3
    ovs_version: "3.4.2-39.el9s"
```

04 프로젝트 수행경과

▶ 수행경과 - DMZ

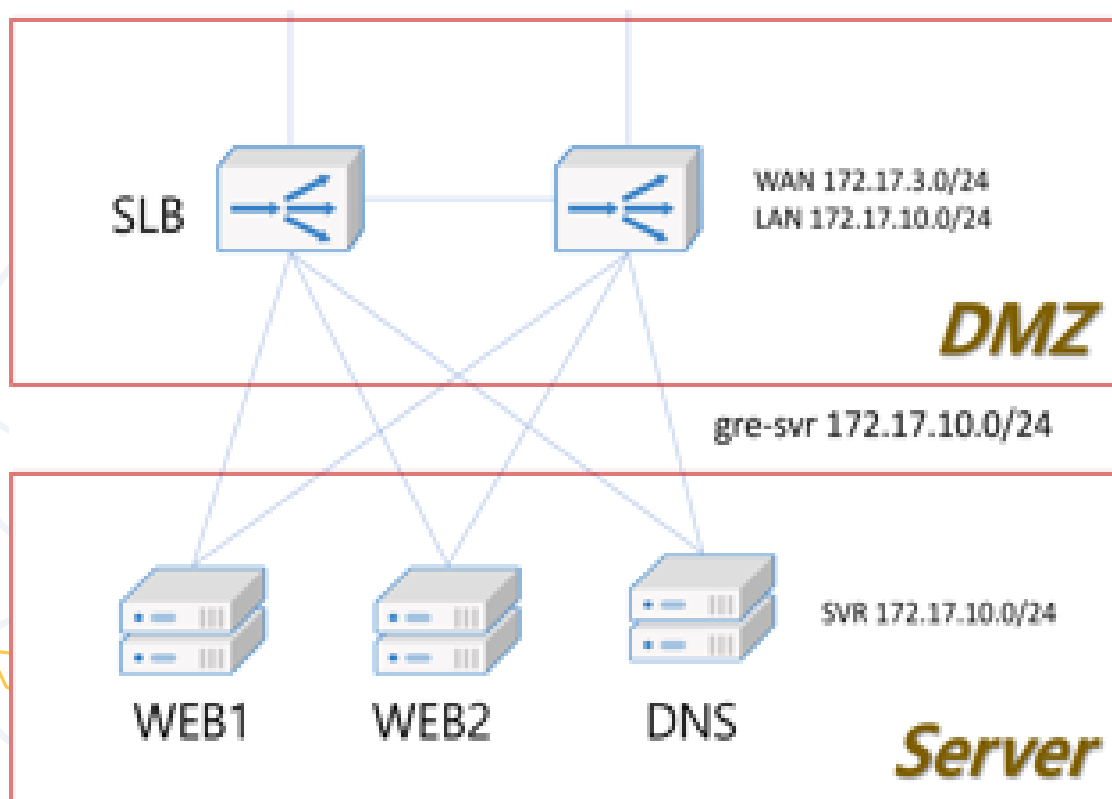
GRE Tunneling 설정(Server 구간)



```
[root@localhost ~]# ovs-vsctl show
a831807f-9ec2-44c5-8eb3-8e067c5dc086
Bridge gre-svr
  Port gre4
    Interface gre4
      type: gre
      options: {key="4", remote_ip="10.201.0.10"}
  Port vnet3
    Interface vnet3
  Port vnet1
    Interface vnet1
  Port gre-svr
    Interface gre-svr
      type: internal
  Port vnet5
    Interface vnet5
ovs_version: "3.4.2-40.el9s"
```

04 프로젝트 수행경과

▶ 수행경과 - DMZ



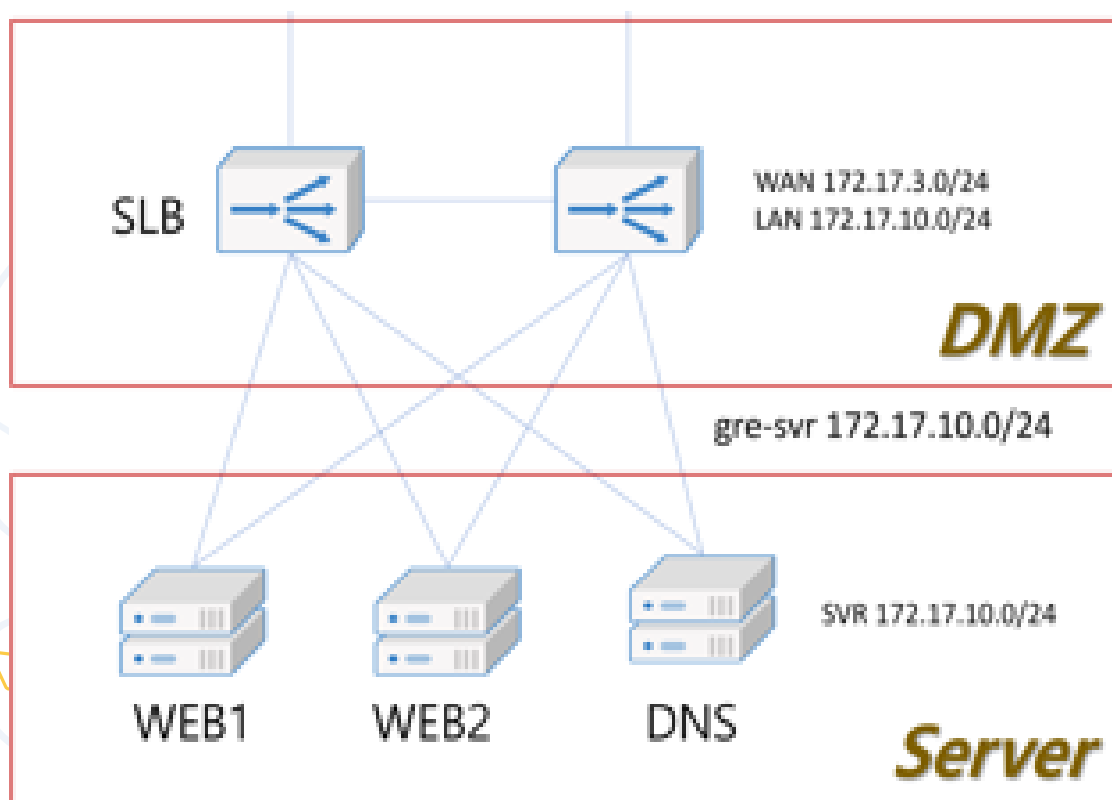
Interface 설정

```
root@localhost:~ — virsh console SLB1
}
interfaces {
  ethernet eth1 {
    address 172.17.3.101/24
    hw-id 52:54:00:d4:4a:0c
  }
  ethernet eth2 {
    address 172.17.10.11/24
    hw-id 52:54:00:6a:ac:b2
  }
  loopback lo {
  }
}
```

```
root@localhost:~ — virsh console SLB2
}
interfaces {
  ethernet eth1 {
    address 172.17.3.102/24
    hw-id 52:54:00:66:7c:ff
  }
  ethernet eth2 {
    address 172.17.10.12/24
    hw-id 52:54:00:86:13:22
  }
  loopback lo {
  }
}
```

04 프로젝트 수행경과

▶ 수행경과 - DMZ



VRRP 설정

```
root@localhost:~ — virsh console SLB1
vyos@SLB1# run sh show vrrp
```

Name	Interface	VRID	State	Priority	Last Transition
10	eth1	10	MASTER	105	1h8m35s
20	eth2	20	MASTER	105	1h8m35s

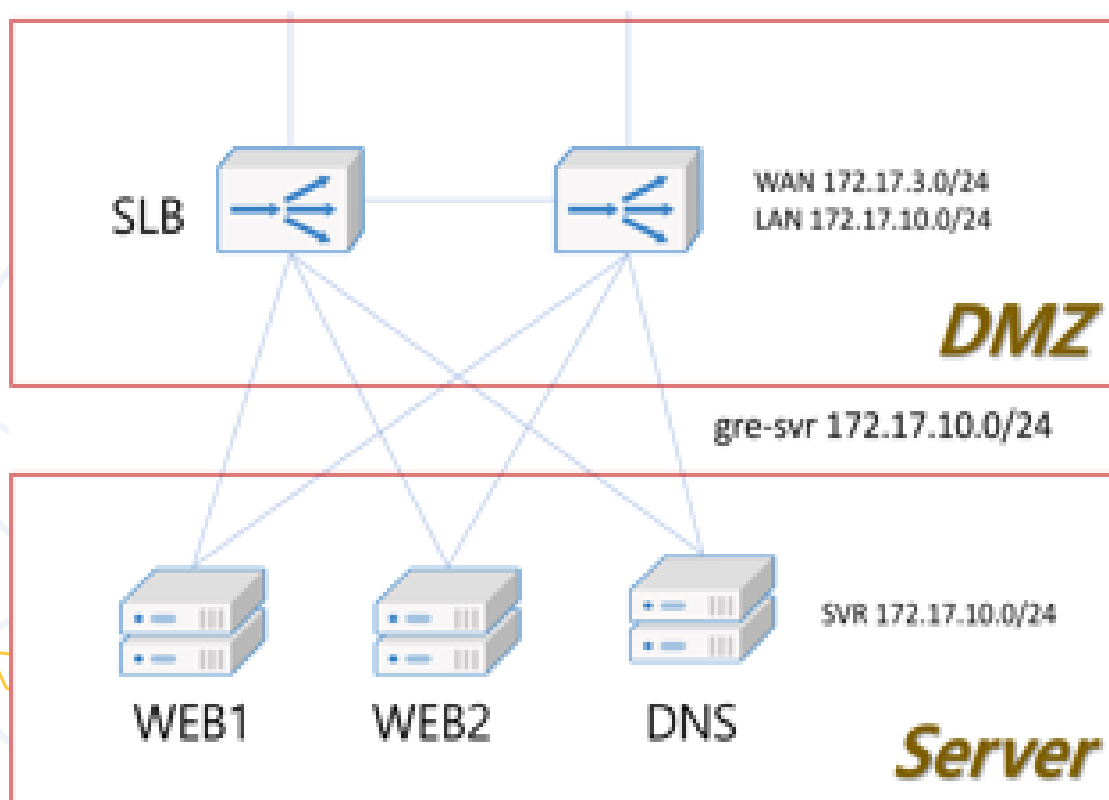
```
root@localhost:~ — virsh console SLB2
vyos@SLB2# run show vrrp
```

Name	Interface	VRID	State	Priority	Last Transition
10	eth1	10	BACKUP	100	1h10m5s
20	eth2	20	BACKUP	100	1h10m5s

04 프로젝트 수행경과

▶ 수행경과 - DMZ

Load Balancing 설정

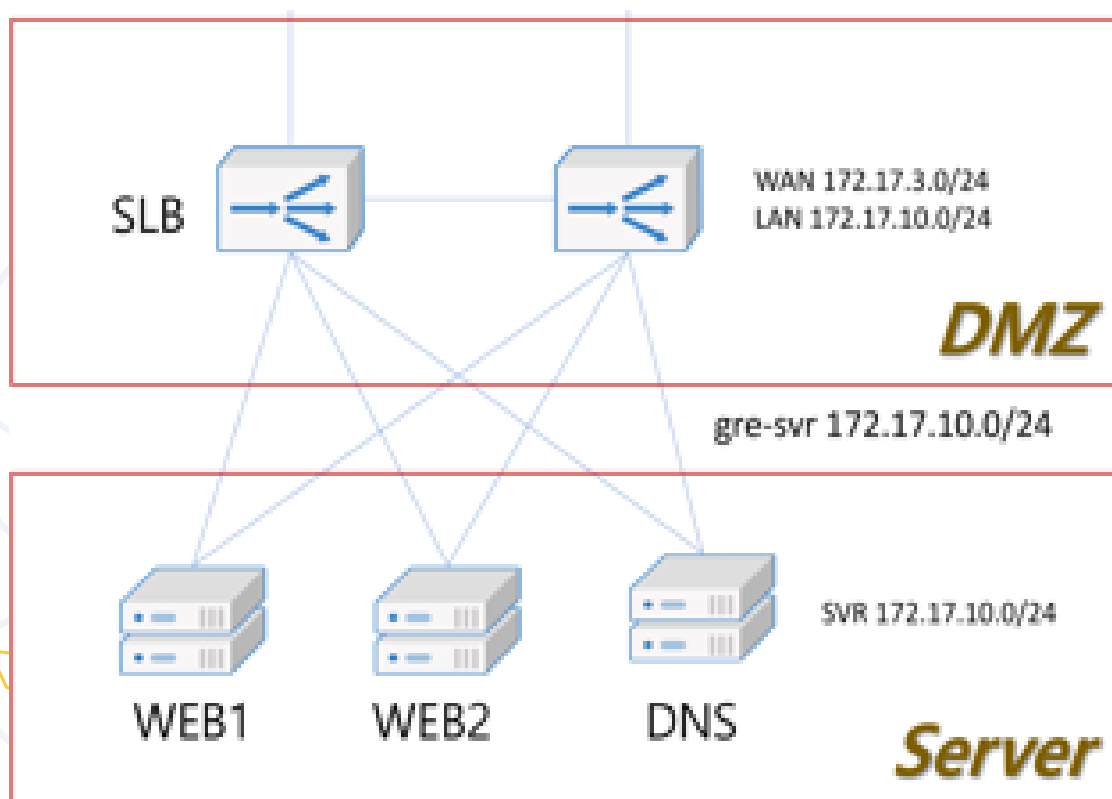


```
root@localhost:~ — virsh console SLB1
load-balancing {
  reverse-proxy {
    backend web-backend {
      balance round-robin
      mode http
      server web1 {
        address 172.17.10.101
        port 80
      }
      server web1-https {
        address 172.17.10.101
        port 443
      }
      server web2 {
        address 172.17.10.102
        port 80
      }
      server web2-https {
        address 172.17.10.102
        port 443
      }
    }
  }
  service http {
    backend web-backend
    listen-address 172.17.10.10
    port 80
  }
  service https {
    backend web-backend
    listen-address 172.17.10.10
    port 443
  }
}
```

```
root@localhost:~ — virsh console SLB2
load-balancing {
  reverse-proxy {
    backend web-backend {
      balance round-robin
      mode http
      server web1 {
        address 172.17.10.101
        port 80
      }
      server web1-https {
        address 172.17.10.101
        port 443
      }
      server web2 {
        address 172.17.10.102
        port 80
      }
      server web2-https {
        address 172.17.10.102
        port 443
      }
    }
  }
  service http {
    backend web-backend
    listen-address 172.17.10.10
    port 80
  }
  service https {
    backend web-backend
    listen-address 172.17.10.10
    port 443
  }
}
```

04 프로젝트 수행경과

▶ 수행경과 - DMZ



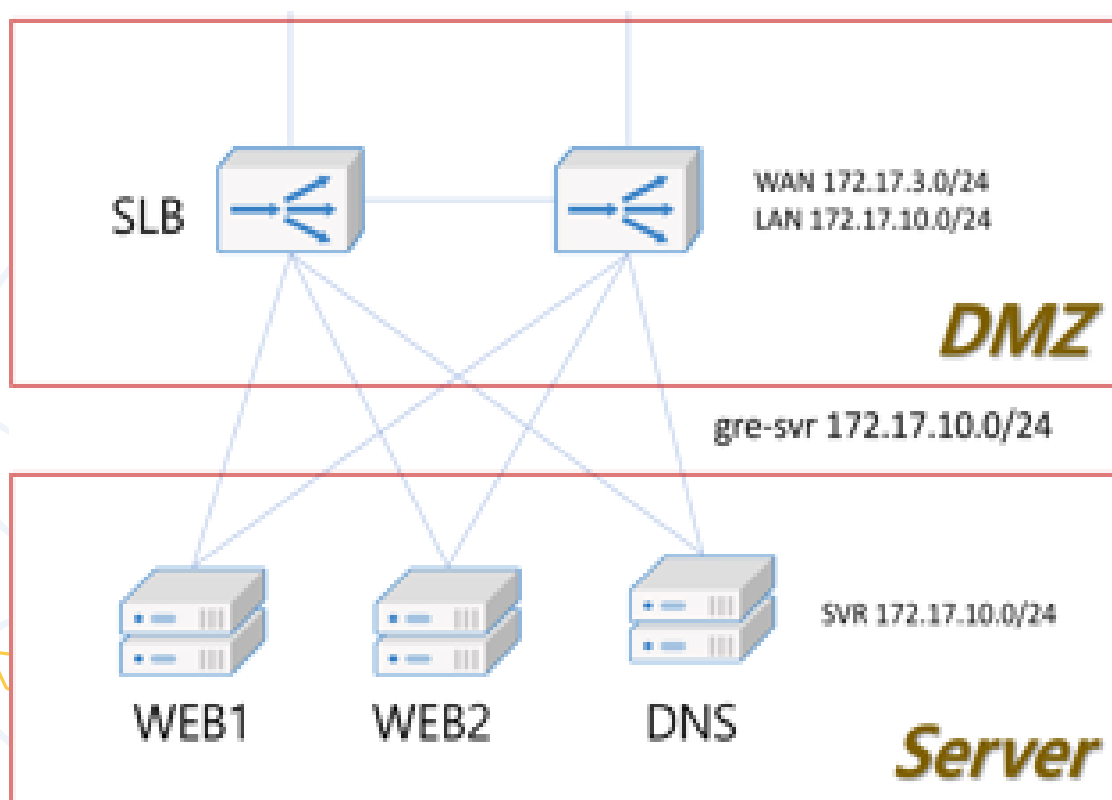
OSPF 설정

```
root@localhost:~ — virsh console SLB1
}
protocols {
  ospf {
    area 0 {
      network 172.17.3.0/24
      network 172.17.10.0/24
    }
    parameters {
      router-id 172.17.10.11
    }
  }
}
```

```
root@localhost:~ — virsh console SLB2
}
protocols {
  ospf {
    area 0 {
      network 172.17.3.0/24
      network 172.17.10.0/24
    }
    parameters {
      router-id 172.17.10.12
    }
  }
}
```


04 프로젝트 수행경과

▶ 수행경과 - DMZ



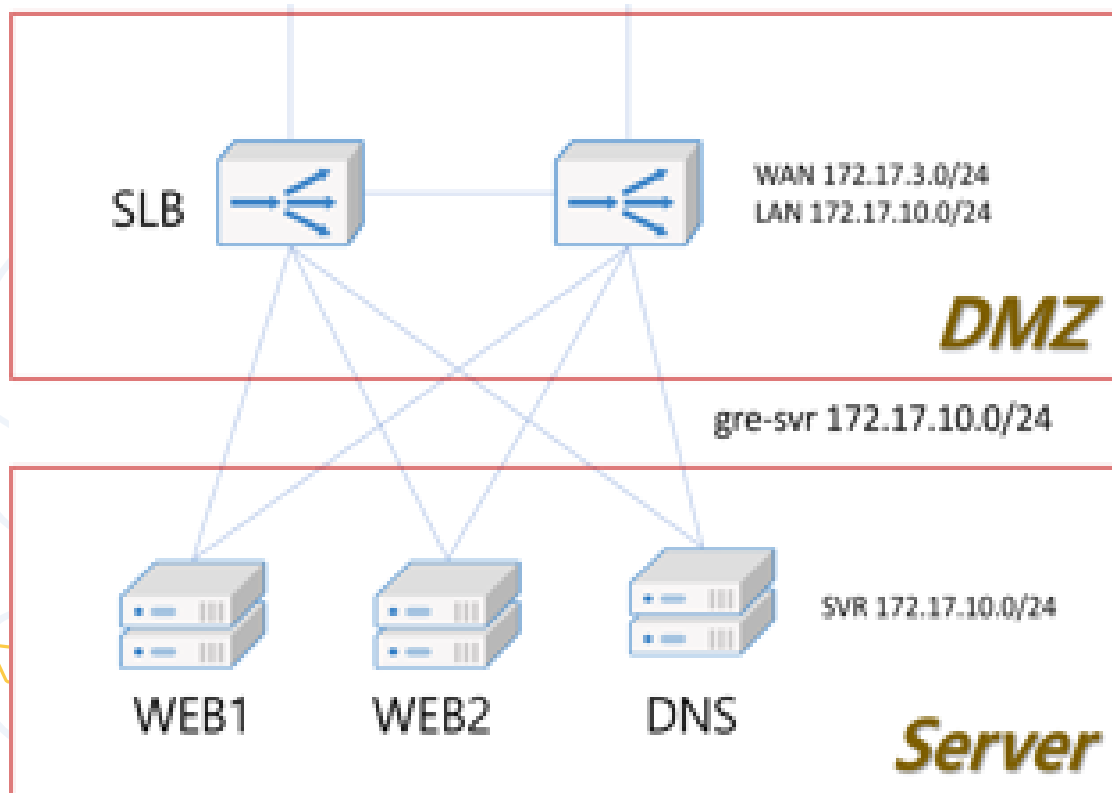
Routing Table 화면

```
root@localhost:~ — virsh console SLB1
vyos@SLB1# run sho ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O>* 0.0.0.0/0 [110/10] via 172.17.3.11, eth1, weight 1, 00:17:08
O>* 10.0.0.0/8 [110/22] via 172.17.3.11, eth1, weight 1, 00:17:09
O>* 172.17.1.0/24 [110/11] via 172.17.3.11, eth1, weight 1, 00:17:19
O>* 172.17.2.0/24 [110/33] via 172.17.3.11, eth1, weight 1, 00:17:09
O  172.17.3.0/24 [110/1] is directly connected, eth1, weight 1, 00:19:09
C>* 172.17.3.0/24 is directly connected, eth1, 01:08:08
O>* 172.17.4.0/24 [110/21] via 172.17.3.11, eth1, weight 1, 00:17:09
O  172.17.10.0/24 [110/1] is directly connected, eth2, weight 1, 01:08:05
C>* 172.17.10.0/24 is directly connected, eth2, 01:08:07
O>* 172.17.100.0/24 [110/43] via 172.17.3.11, eth1, weight 1, 00:17:09
O>* 172.17.200.0/24 [110/43] via 172.17.3.11, eth1, weight 1, 00:17:09
O>* 192.168.50.0/24 [110/20] via 172.17.3.11, eth1, weight 1, 00:17:08
O>* 192.168.51.0/24 [110/53] via 172.17.3.11, eth1, weight 1, 00:17:09
```

04 프로젝트 수행경과

▶ 수행경과 - DMZ



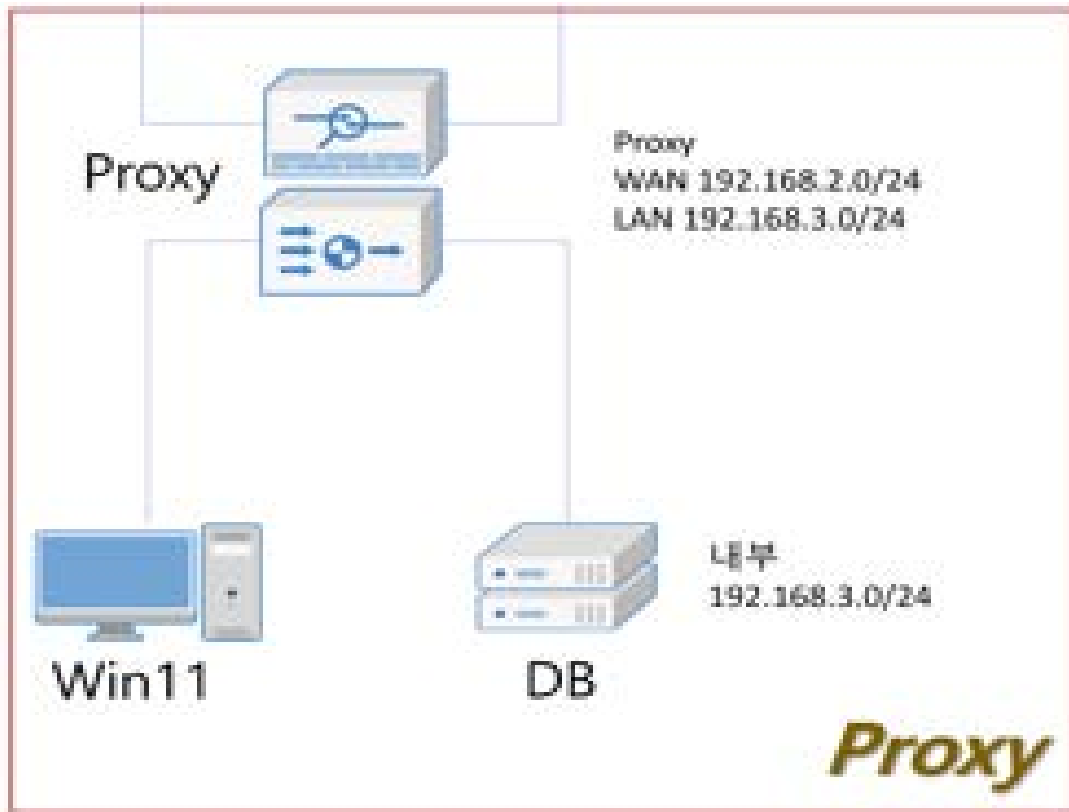
DNS 서버 설정

```
root@localhost:~ — /usr/bin/vim /var/named/nonblindsite.com...
$TTL 3H
@      IN SOA  nonblindsite.com. nonblindsite.com. (
                                0      ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum

NS     @
A      172.17.10.150
www    A      172.17.10.101
www    A      172.17.10.102
www    A      172.17.10.103
AAAA   ::1
```

04 프로젝트 수행경과

▶ 수행경과 - Proxy

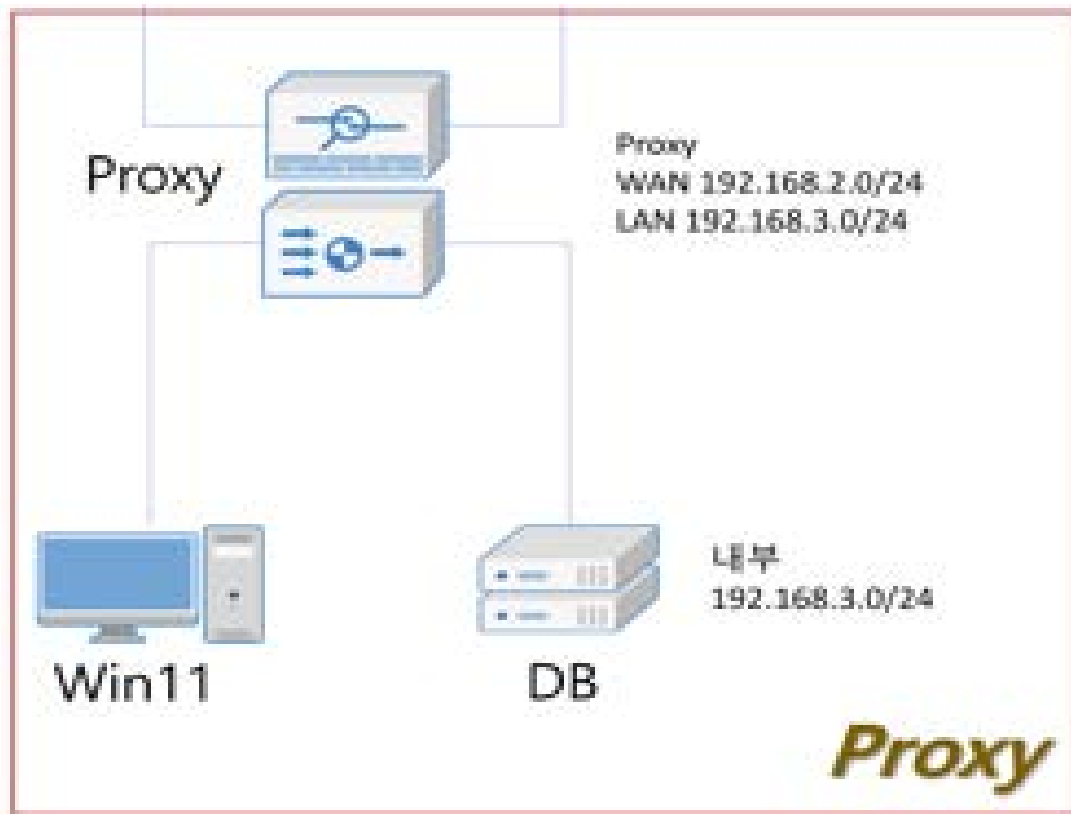


- FireWall과 GRE Tunneling
- Static Routing 설정
- DB server, Window11 사용자 PC
- Transparent Proxy 설정

04 프로젝트 수행경과

▶ 수행경과 - Proxy

GRE Tunneling 설정

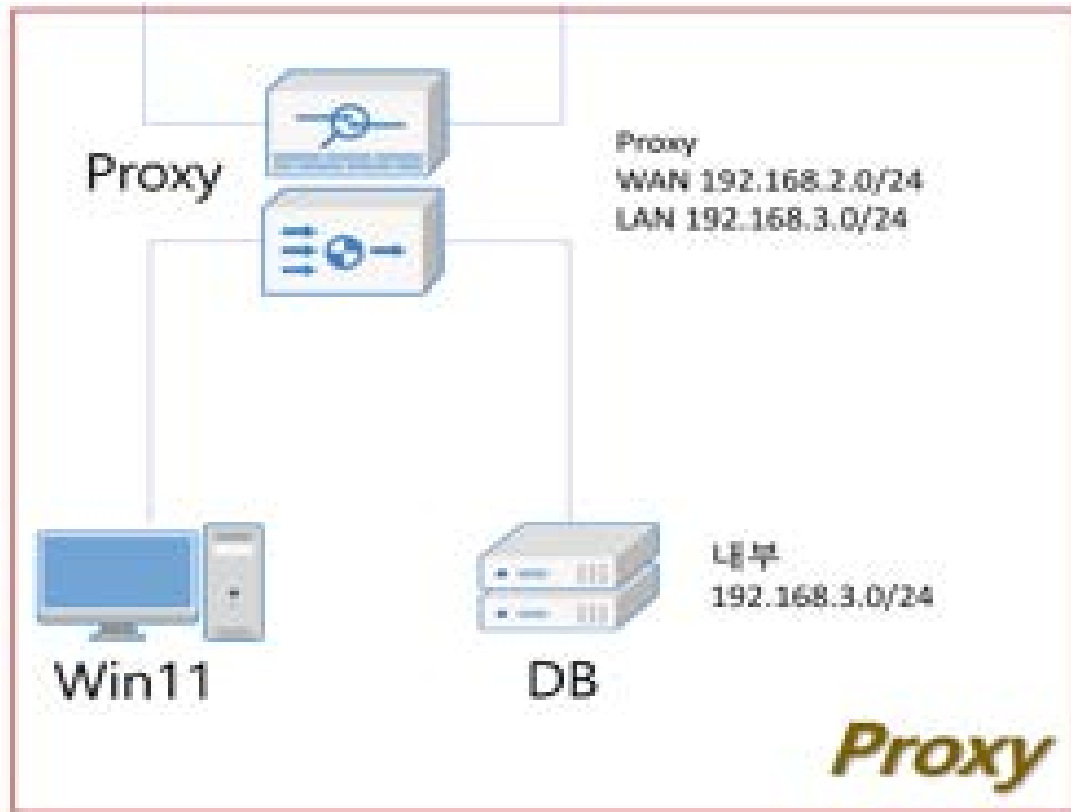


```
b8f2e2f2-d159-4115-be78-0fce5808a356
Bridge gre-proxy
Port gre-proxy
Interface gre-proxy
    type: internal
Port gre2
Interface gre2
    type: gre
    options: {key="2", remote_ip="10.201.0.2"}
Port vnet0
Interface vnet0
ovs_version: "3.4.2-41.el9s"
```

04 프로젝트 수행경과

▶ 수행경과 - Proxy

Static Routing 설정



Routing: STATIC

General Routes

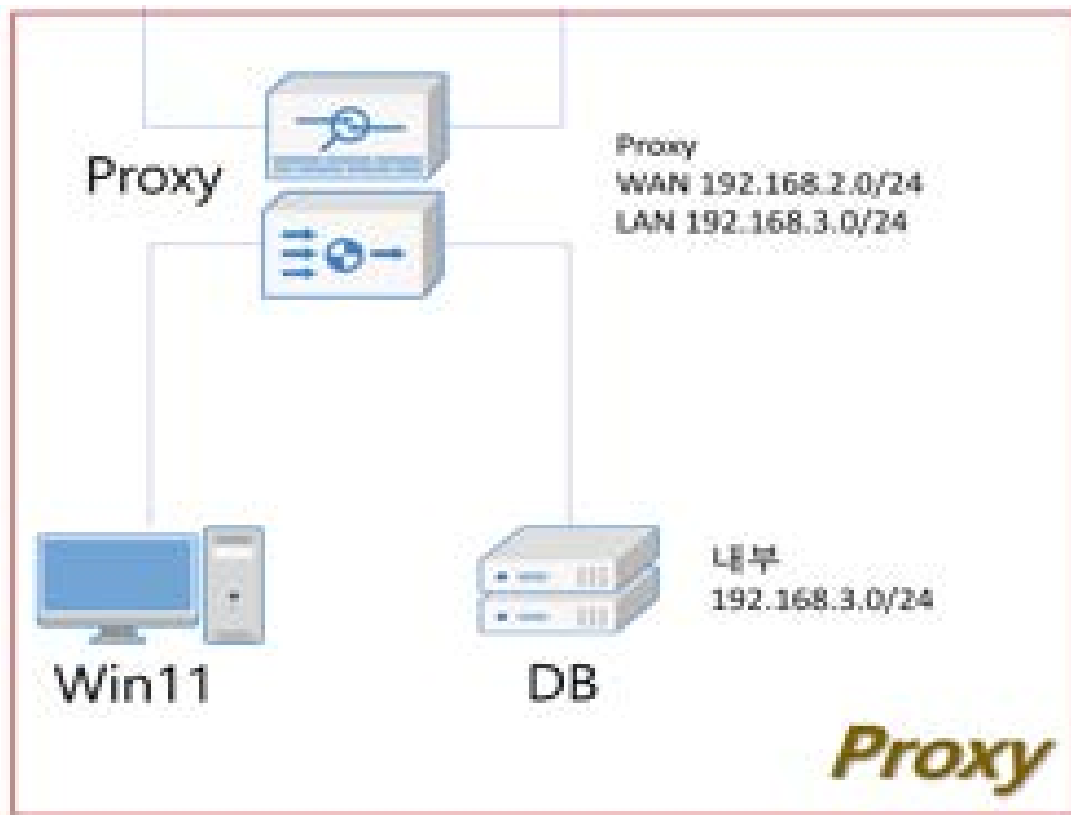
<input type="checkbox"/> Enabled	Network	Gateway	Interface	Commands
<input checked="" type="checkbox"/>	0.0.0.0/0	192.168.2.10	WAN	

Showing 1 to 1 of 1 entries

04 프로젝트 수행경과

▶ 수행경과 - Proxy

DB server 설정



```
MariaDB [team1] > show tables
-> ;
+-----+
| Tables_in_team1 |
+-----+
| users           |
+-----+
1 row in set (0.000 sec)

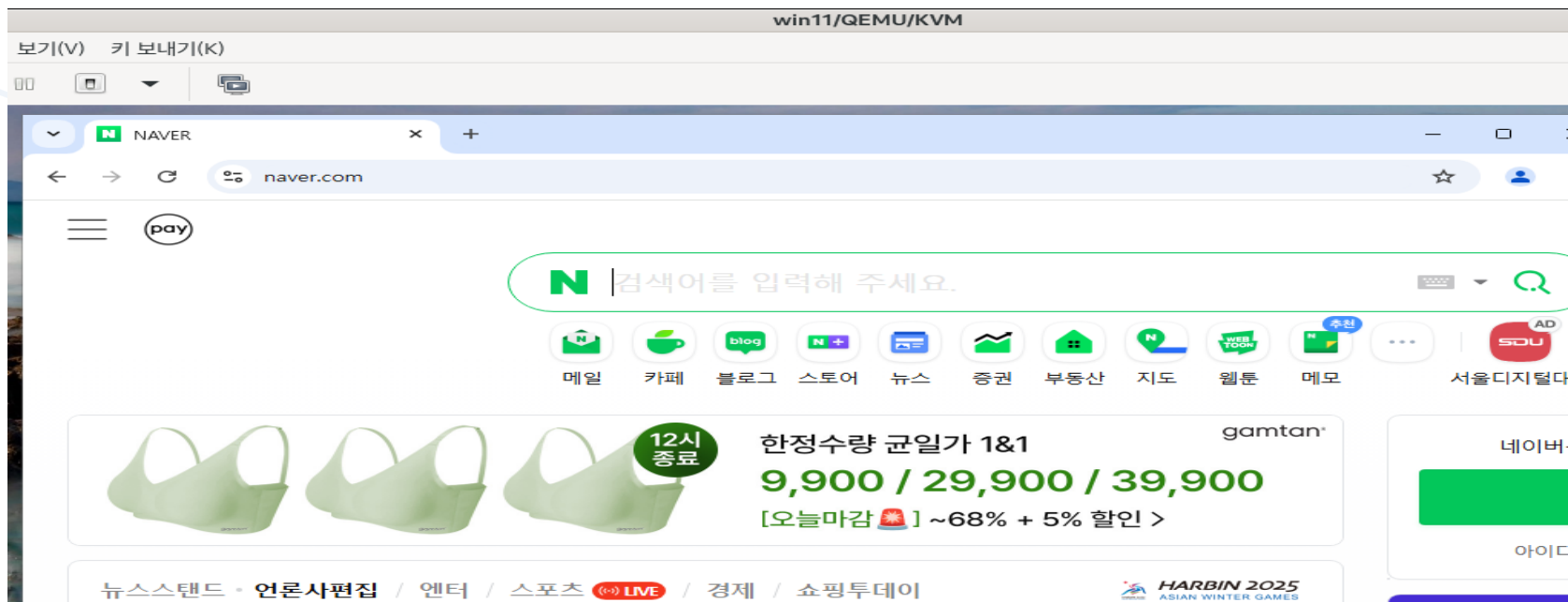
MariaDB [team1] > select * from users;
+----+-----+-----+-----+
| id | name | age | email                |
+----+-----+-----+-----+
| 1  | Alice | 25  | alice@example.com    |
| 2  | Bob   | 30  | bob@example.com      |
+----+-----+-----+-----+
2 rows in set (0.012 sec)

MariaDB [team1] > SHOW GRANTS FOR 'team1'@'%';
+-----+
| Grants for team1@% |
+-----+
| GRANT ALL PRIVILEGES ON *.* TO 'team1'@'%' IDENTIFIED BY PASSWORD '*FABE5482D5AADF36D028AC443D117BE1180B9725' WITH GRANT OPTION |
+-----+
```

04 프로젝트 수행경과

▶ 수행경과 - 테스트 화면

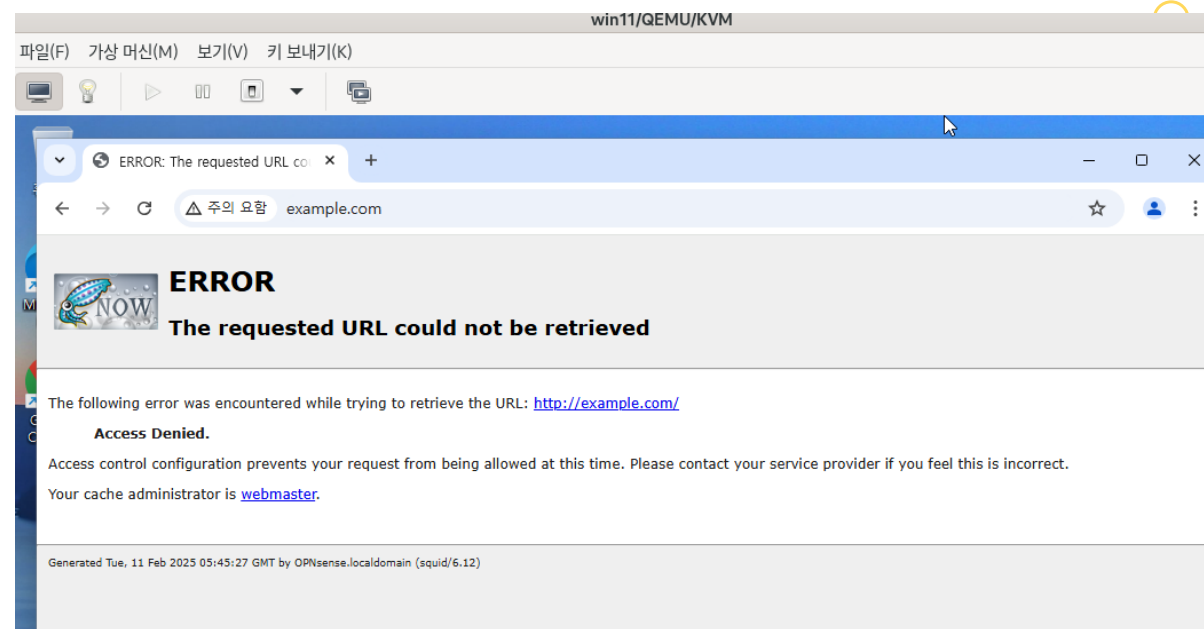
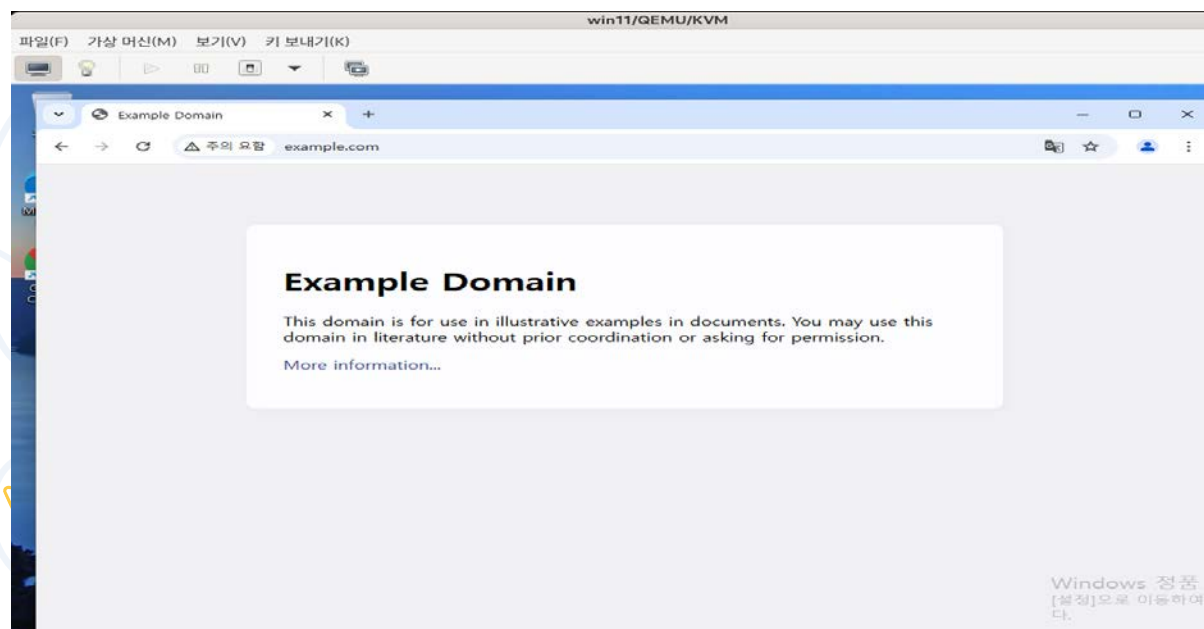
내부 Win 11 PC에서 외부 www.naver.com 사이트 접속 화면



04 프로젝트 수행경과

▶ 수행경과 - 테스트 화면

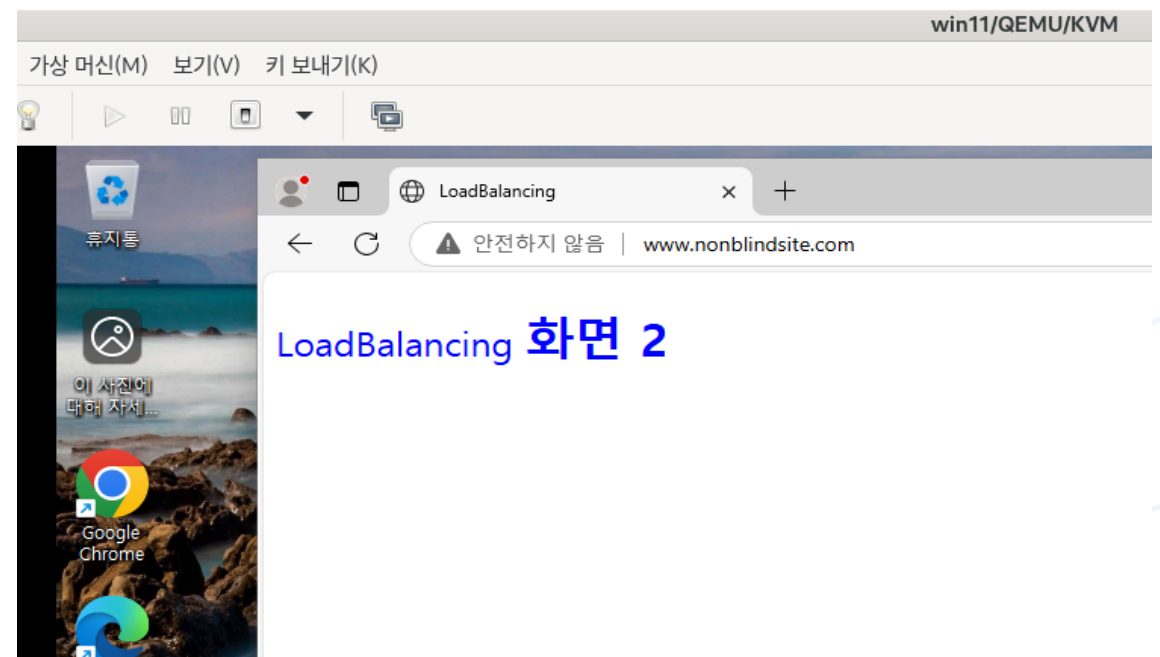
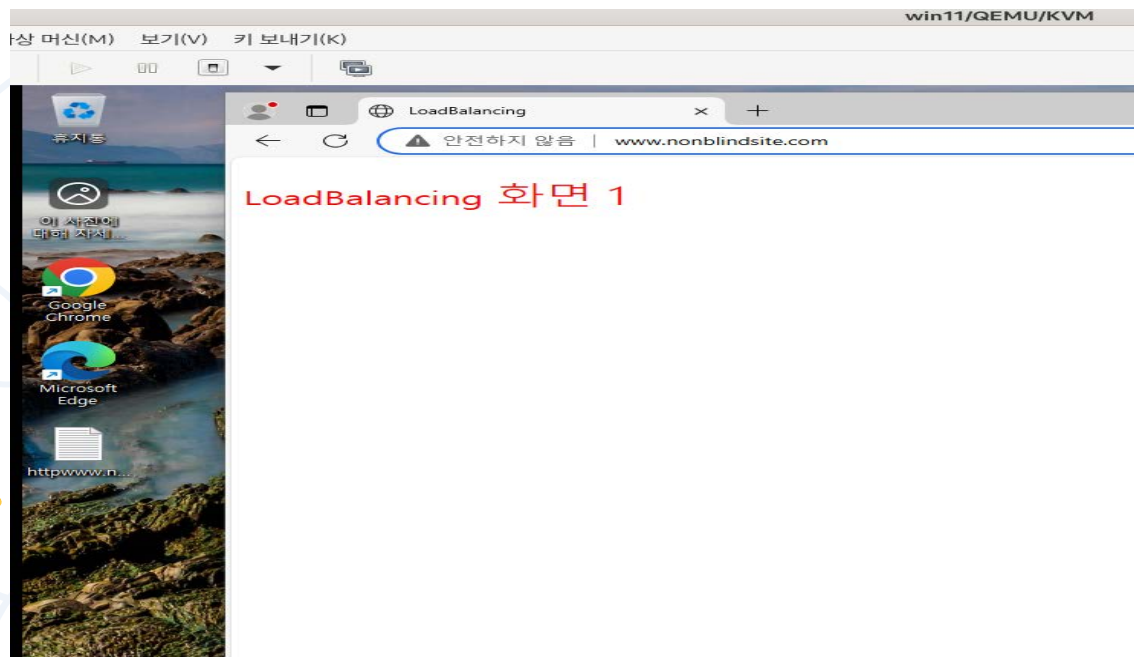
Transparent Proxy에서 특정 사이트 접근 차단 화면



04 프로젝트 수행경과

▶ 수행경과 - 테스트 화면

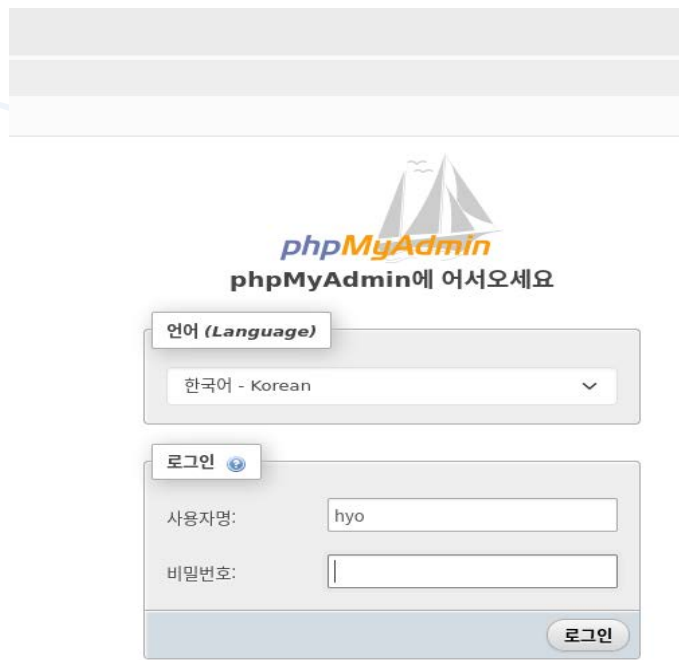
Win 11을 통한 www.nonblindsite.com 웹서버 접속 및 Load Balancing 화면



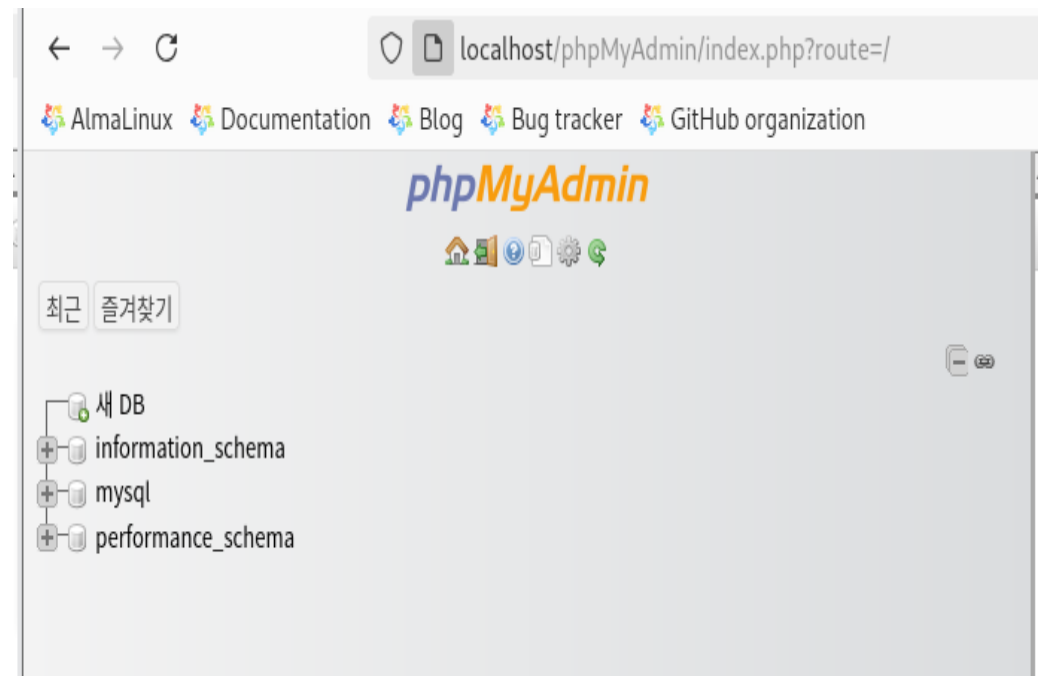
04 프로젝트 수행경과

▶ 수행경과 - 테스트 화면

DMZ Web server에서 Proxy DB server 접속 화면



The image shows the phpMyAdmin login interface. At the top, there is a logo with a sailboat and the text "phpMyAdmin" and "phpMyAdmin에 어서오세요". Below this, there is a language selection dropdown menu labeled "언어 (Language)" with "한국어 - Korean" selected. Underneath is a login section labeled "로그인" with fields for "사용자명:" (username) containing "hyo" and "비밀번호:" (password) which is empty. A "로그인" button is at the bottom right of the login section.



04 프로젝트 수행경과

▶ 수행경과 – 테스트 화면

Surikata 테스트 특정 IP 차단 화면

```
root@OPNsense:/usr/local/etc/suricata/rules # ping 10.10.10.16
PING 10.10.10.16 (10.10.10.16): 56 data bytes
64 bytes from 10.10.10.16: icmp_seq=0 ttl=127 time=3.080 ms
64 bytes from 10.10.10.16: icmp_seq=1 ttl=127 time=0.987 ms
^C
--- 10.10.10.16 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.987/2.034/3.080/1.047 ms
root@OPNsense:/usr/local/etc/suricata/rules # ping 10.10.10.16
PING 10.10.10.16 (10.10.10.16): 56 data bytes
```

Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
2025-02-12T00:30:35.394551+0000	429496...	blocked	wan	10.10.10.16	0	172.17.4.100	0	host_access	
2025-02-12T00:30:35.394551+0000	429496...	blocked	wan	10.10.10.16	0	172.17.4.100	0	host_access	
2025-02-12T00:29:34.629603+0000	429496...	allowed	wan	10.10.10.16	0	172.17.4.100	0	host_access	

Showing 1 to 3

04 프로젝트 수행경과

▶ 수행경과 – 테스트 화면

Surikata 테스트 Land Attack 공격 탐지 화면

```
(root@kali)-[/home/kali]
# hping3 -S -p 80 -a 172.17.10.10 172.17.10.10 --flood
HPING 172.17.10.10 (eth0 172.17.10.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 172.17.10.10 hping statistic —
75951 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
2025-02-11T07:28:58.262475+0000	1000005	allowed	lan	172.17.10.10	18180	172.17.10.10	80	LAND Attack Detected	
2025-02-11T07:28:58.217710+0000	1000005	allowed	lan	172.17.10.10	17914	172.17.10.10	80	LAND Attack Detected	
2025-02-11T07:28:58.217710+0000	1000005	allowed	lan	172.17.10.10	17913	172.17.10.10	80	LAND Attack Detected	
2025-02-11T07:28:58.217710+0000	1000005	allowed	lan	172.17.10.10	17912	172.17.10.10	80	LAND Attack Detected	
2025-02-11T07:28:58.217710+0000	1000005	allowed	lan	172.17.10.10	17911	172.17.10.10	80	LAND Attack Detected	
2025-02-11T07:28:58.217710+0000	1000005	allowed	lan	172.17.10.10	17910	172.17.10.10	80	LAND Attack Detected	
2025-02-11T07:28:58.217710+0000	1000005	allowed	lan	172.17.10.10	17909	172.17.10.10	80	LAND Attack Detected	

« 1 2 »

Showing 1 to 7

04 프로젝트 수행경과

▶ 수행경과 – 테스트 화면

Surikata 테스트 스텔스 포트 스캔 탐지 및 차단 화면

```
(root@kali)-[/home/kali]
# sudo nmap -sS -p 80 172.17.10.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-11 02:48 EST
Nmap scan report for www.nonblindsite.com (172.17.10.10)
Host is up (0.0083s latency).
```

```
PORT      STATE SERVICE
80/tcp    open  http
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
2025-02-11T07:48:48.141594+0000	1000001	allowed	wan	172.17.4.200	35247	172.17.10.10	80	Nmap SYN Scan detected	
2025-02-11T07:48:47.477879+0000	1000001	allowed	lan	172.17.4.200	35592	172.17.10.10	443	Nmap SYN Scan detected	
2025-02-11T07:48:46.733375+0000	1000001	allowed	wan	172.17.4.200	48125	172.17.10.10	443	Nmap SYN Scan detected	

« < 1 > »

Showing 1 to 3

Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
2025-02-11T08:18:05.693047+0000	1000001	blocked	lan	172.17.1.199	36426	172.17.1.100	80	Nmap SYN Scan detected	
2025-02-11T08:18:05.693047+0000	1000001	blocked	lan	172.17.1.199	36426	172.17.1.100	80	Nmap SYN Scan detected	
2025-02-11T08:11:48.242721+0000	1000001	blocked	lan	172.17.10.101	40132	34.117.188.166	443	Nmap SYN Scan detected	
2025-02-11T08:11:48.242721+0000	1000001	blocked	lan	172.17.10.101	40132	34.117.188.166	443	Nmap SYN Scan detected	
2025-02-11T08:11:46.330155+0000	1000001	blocked	lan	172.17.10.150	55183	192.55.83.30	53	Nmap SYN Scan detected	
2025-02-11T08:11:46.330155+0000	1000001	blocked	lan	172.17.10.150	55183	192.55.83.30	53	Nmap SYN Scan detected	
2025-02-11T08:11:44.370378+0000	1000001	blocked	lan	172.17.10.150	53011	192.41.162.30	53	Nmap SYN Scan detected	

04 프로젝트 수행경과

▶ 수행경과 – 테스트 화면

Surikata 테스트 ICMP ping Flood 차단 화면



```
(root@kali)-[/home/kali/.cache]
# hping3 --icmp --flood -c 25 172.17.10.10
HPING 172.17.10.10 (eth0 172.17.10.10): icmp mode set, 28 headers + 0 data by
tes
hping in flood mode, no replies will be shown
^C
— 172.17.10.10 hping statistic —
256558 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
2025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	
2025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	
2025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	
2025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	
2025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	
2025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	
2025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	

« ‹ 1 2 › »

Showing 1 to 7

04 프로젝트 수행경과

▶ 수행경과 – 시연 영상

proxy 시연영상 (특정 사이트 도메인 차단)

<https://drive.google.com/file/d/1U8jwJYfe4PkFQilN01V9KRAVGoxKosji/view?usp=sharing>

04 프로젝트 수행경과

▶ 수행경과 - 시연 영상

SLB 시연영상1 (내부-웹 접속)

https://drive.google.com/file/d/1zjEFkxxRVy_kCZG2FMkE_fcdaDizZQr-/view?usp=sharing

04 프로젝트 수행경과

▶ 수행경과 - 시연 영상

SLB 시연영상2 (외부-웹 접속)

https://drive.google.com/file/d/1fl0n6isf_2kSJ8xpQyBf0WlkKi6lyjnk/view?usp=sharing

04 프로젝트 수행경과

▶ 수행경과 – 시연 영상

IPS 탐지 시연 영상

<https://drive.google.com/file/d/1feIOKM6E-PeJZNj324FYn5toi45VhRly/view?usp=sharing>

05 기대 효과

▶ 기대효과

1. 보안 강화

- 방화벽, IDS/IPS, 프록시를 통해 외부 공격 및 내부 보안 위협을 최소화함

2. 가용성 향상

- SLB를 통해 네트워크 및 서비스 부하를 효과적으로 관리하여 장애 발생 가능성을 낮춤

3. 확장성 보장

- KVM 가상화 기반의 백본망 구축을 통해 향후 CCTV 네트워크 및 보안 정책 확장이 용이함

4. 데이터 무결성 확보

- 내부망을 보호하고, 접근 통제를 강화하여 감시 데이터의 안전성을 유지함

5. 네트워크 최적화

- 적절한 보안 정책 적용과 트래픽 관리 기능을 통해 CCTV 서비스의 품질을 극대화함

05 소감

권호중

이번 KVM 기반 온프레미스 인프라 구축 프로젝트는 처음부터 끝까지 도전의 연속이었습니다. 특히 방화벽(Firewall) 설정 과정에서 보안 정책을 최적화하는 데 많은 고민이 필요했고, 다양한 테스트를 거치며 안정적인 구성을 완성할 수 있었습니다. 또한, 발표 자료를 작성하면서 프로젝트의 핵심 내용을 정리하고 공유하는 과정에서 많은 것을 배우게 되었습니다. 최종적으로 모든 시스템이 원활하게 동작하는 모습을 보면서 큰 보람을 느꼈고, 이번 경험을 통해 더욱 성장할 수 있었습니다.

지승헌

이번 프로젝트에서 프록시(Proxy) 서버를 구성하고 최적화하는 작업을 맡았는데, 이를 통해 네트워크 트래픽 제어와 보안 강화에 대한 실무적인 경험을 쌓을 수 있었습니다. 특히, 방화벽 및 IPS와의 연동을 고려하며 설정하는 과정에서 다양한 시행착오를 겪었지만, 결국 안정적인 구성을 완성할 수 있었습니다. 또한, 프로젝트 산출물을 작성하며 전체적인 흐름을 정리하는 과정이 매우 유익했습니다. 이번 프로젝트를 통해 시스템 설계 및 운영 능력을 한 단계 더 성장시킬 수 있었고, 향후 더욱 복잡한 환경에서도 자신감을 갖고 도전할 수 있을 것 같습니다.

이효운

이번 프로젝트에서 SLB(서버 부하 분산)를 구성하는 작업을 맡았는데, 이 과정에서 부하 분산 알고리즘과 네트워크 트래픽 관리에 대한 이해도를 한층 높일 수 있었습니다. 특히, 예상치 못한 트래픽 병목 현상을 해결하기 위해 여러 가지 설정을 테스트하고 최적의 방안을 도출하는 과정이 인상적이었습니다. 팀원들과 협업하며 문제를 해결해 나가는 과정이 매우 의미 있었고, 보고서를 작성하며 프로젝트를 돌아보는 기회를 가질 수 있었습니다. 이번 프로젝트를 통해 실무적인 경험을 쌓으며, 앞으로 더 복잡한 환경에서도 자신 있게 SLB를 설계할 수 있을 것 같습니다.

연광흠

IPS & IDS 구축을 담당하며 보안 시스템의 중요성을 다시 한번 실감한 프로젝트였습니다. 실시간으로 위협을 탐지하고 대응할 수 있도록 설정하는 과정에서 많은 실험과 조정을 거쳐야 했지만, 최종적으로 안정적인 구성을 완료했을 때의 성취감은 이루 말할 수 없었습니다. 프로젝트가 끝나고 네트워크 보안이 정상적으로 동작하는 모습을 보니 그동안의 노력이 헛되지 않았다는 걸 느꼈습니다. 특히, 이번 경험을 통해 보안 시스템을 더욱 깊이 있게 이해할 수 있었고, 실전 경험을 쌓을 수 있어 정말 뜻깊은 프로젝트였습니다.