

결 재	담당	원장

클라우드 컴퓨팅과 보안솔루션을 활용한 DC 엔지니어 양성

2차 프로젝트 완료 보고서

CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축

2025.02.04

구성원 : 권효중
지승헌
이효운
연광흠

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

문서 개정 이력

개정번호	개정일자	시행일자	개정내용	담당자
1.0	2025.01.20	2025.02.04	최초 작성	지승헌
1.1	2025.02.03.	2025.02.04	중간 수정	지승헌
1.2	2025.02.04.	2025.02.04.	최종 완료	지승헌

교

육

기

관

:

한

국

정

보

교

육

원

팀

명

:

1

조

팀

원

:

권

효

중

팀

원

:

지

승

헌

팀

원

:

이

효

원

팀

원

:

연

광

흙

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

목차

1. 프로젝트 개요

- 프로젝트 명 4
- 프로젝트 기간 4
- 프로젝트 목표 4
- 프로젝트 시나리오 4
- 프로젝트 수행 요건 4

2. 프로젝트 추진 체계

- 프로젝트 참여 인력 총괄표 5
- 참여 인력 업무 분장 5

3. 세부 프로젝트 내용

- 전체 구성도 6
- 각 네트워크 구성도 7
- 서버(가상) 구성 현황 9
- 네트워크 구성 현황 10
- 상세 구축 및 구성 내용 26
- 구축 결과 31

4. 개별 후기 40

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

1. 프로젝트 개요

- 프로젝트 명

네트워크 프로젝트 2차 - CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축

- 프로젝트 기간

2025.01.16.- 2025.02.04

- 프로젝트 목표

가) KVM으로 구현한 온 프레미스 설계

나) OVS_GRE 와 FireWall, IPS & IDS, Proxy 그리고 SLB 구현

- 프로젝트 시나리오

가) 가정

- CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축 - 'Non Blind Site(NBS)'

나) 세부내용

1. 현대 CCTV 보안 시스템은 단순한 영상 감시를 넘어, 실시간 데이터 분석 및 인공지능 기반 탐지 기능까지 요구하는 실정
2. 이러한 환경에서 네트워크 보안과 가용성이 핵심 요소로 작용하며, 안정적인 서비스 제공을 위한 백본망 구축 및 고도화된 보안 정책이 필수
3. 'Non Blind Site(NBS)'라는 KVM 가상화 기반의 백본망을 구축하여, 보안 장비와 네트워크 서비스가 유기적으로 연동될 수 있도록 시나리오 설계
4. 'Non Blind Site(NBS)'라는 백본망에 방화벽(Firewall), IDS/IPS, 프록시(Proxy), SLB(부하 분산) 등의 보안 기능을 구현하여, 내·외부 네트워크 및 서버 존의 보안을 강화 및, 신뢰성 높은 서비스 환경을 조성하는 것이 핵심 목표
5. 이를 통해, CCTV 영상 및 관련 서비스 데이터를 안전하게 보호하고, 내부 네트워크의 보안성을 극대화하며, 원활한 트래픽 관리를 통해 고성능의 감시 시스템을 구현

- 프로젝트 수행요건

가) 하이퍼 바이저를 활용한 온프레미스 설계

- KVM을 사용하여 보안장비 및 서비스가 포함된 백본망 구축한다
- FireWall 기능을 구현하여 내부, 외부 및 서버존 구축과 적합한 보안정책 및 기능을 설정
- Proxy 기능을 구현하고, 구성에 적합한 보안정책 및 기능을 설정한다. (테스트 첨부).
- IDS/IPS 기능을 구현하고 구성에 적합한 보안정책 및 기능을 설정한다. (SURICATA 정책 5가지)
- SLB 기능을 구현하고 3종류 이상의 서비스를 구축한다. (3종 이상의 서비스 구현)

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

2. 프로젝트 추진 체계

● 프로젝트 참여 인력 총괄표

성명	소속	역할	담당업무
권효중	한국정보교육원	Project Manager FireWall	FireWall 구축 및 발표 자료 작성
이효운	한국정보교육원	Project Leader SLB	SLB 구축 및 보고서 작성
연광흠	한국정보교육원	Project Leader IPS & IDS	IPS 구축 및 보고서 작성
지승헌	한국정보교육원	Project Leader Proxy	Proxy 구축 및 보고서 작성, 산출물 작성

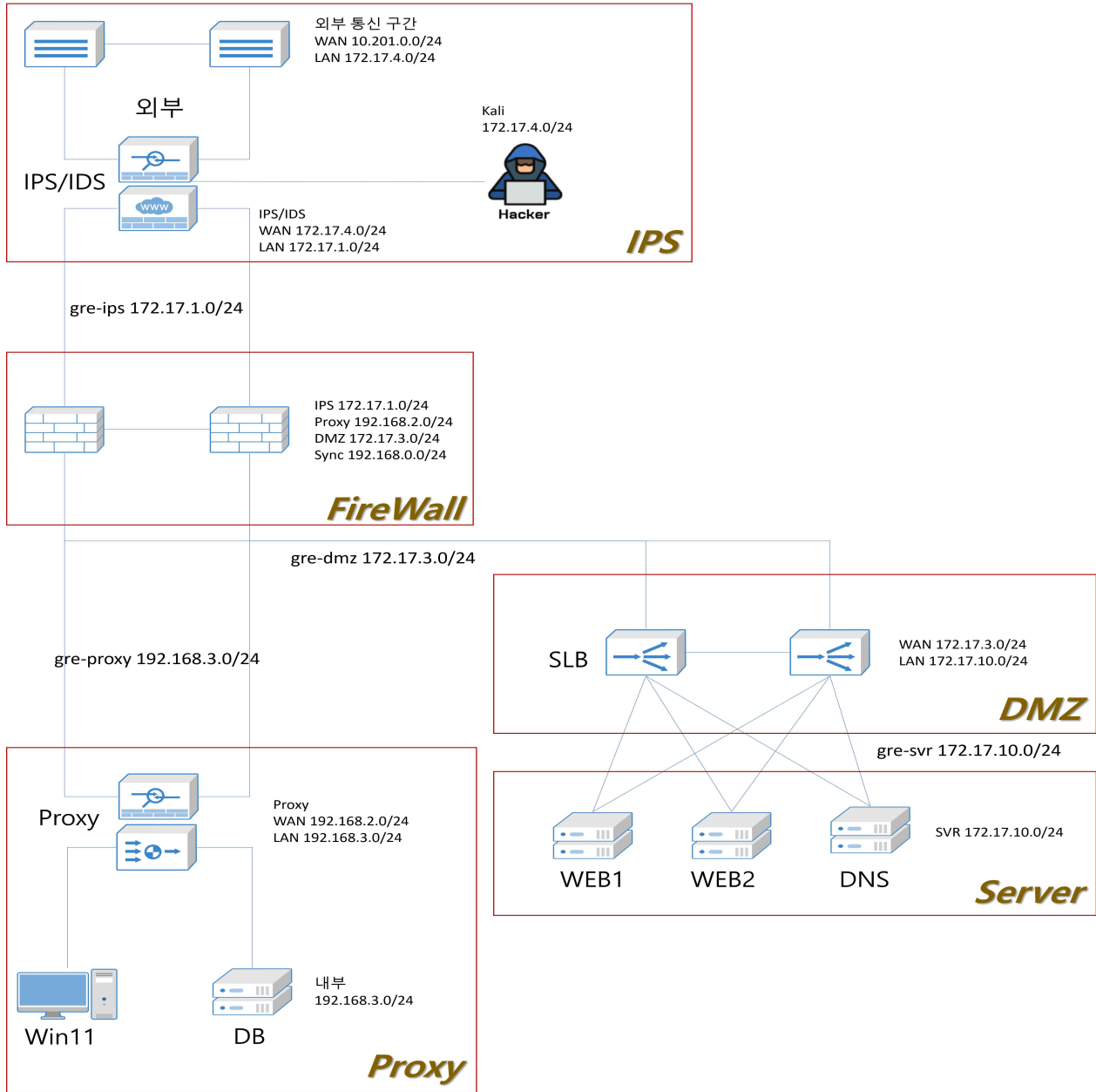
● 참여 인력 업무 분담

업무명	업무내용
보고서 작성	<ul style="list-style-type: none"> - 프로젝트 기획서 작성 - 프로젝트 결과 보고서 작성 - 프로젝트 진행 상황에 대한 일정 조정 - 기타 보고서 작성 및 발표 진행
온프레미스 토폴로지 구성	<ul style="list-style-type: none"> - 네트워크 토폴로지 구성 - 네트워크 장비 수 산정 및 배분 - 외부망과 사설망의 분리
네트워크 구성	<ul style="list-style-type: none"> - 외부와 내부망 사이의 네트워크 구성 - OVS_GRE 터널링 구성 - OSPF 구성 - NAT 구성 - Static 라우팅 구성
보안 구현	<ul style="list-style-type: none"> - IPS & IDS 구현 - FireWall 구현 - Proxy 구현 - SLB 구현 - 공격자 테스트

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

3. 세부 프로젝트 내용

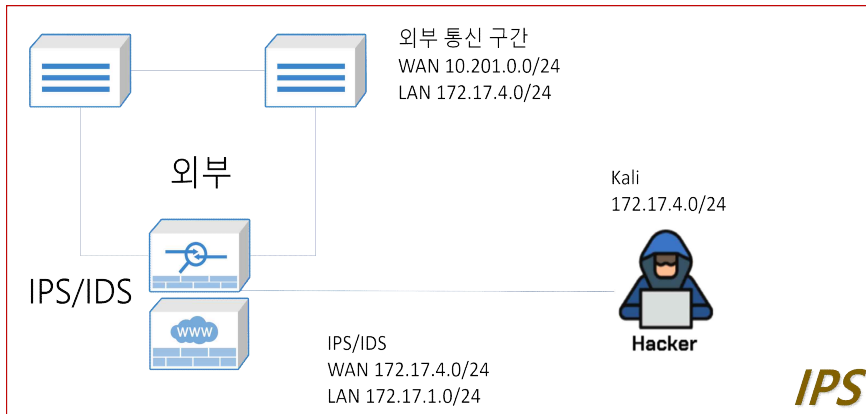
● 전체 구성도



- 1) KVM 기반, 'IPS & IDS', 'FireWall', 'Proxy', 'SLB' 총 4개의 구역으로 나누어진 온프레미스 환경
- 2) 각 구역은 서로 다른 IP 대역을 가지고 있으며, OVS_GRE를 통한 터널링
- 3) G/W, FireWall 이중화 및 SLB를 통해 부하 분산 및 안정적 환경 구성
- 4) IPS & IDS와 FireWall, Proxy를 통한 보안 강화 구현
- 5) IPS 구역에 침입한 가상의 공격자 Kali를 통한 보안 테스트 환경 조성

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

● IPS & IDS 구성도



IPS VM
BR1 10.201.0.16/16
Gre-ips 172.17.1.199/24

gre-ips 172.17.1.0/24

● FireWall 구성도

GRE구간

Gre-ips 172.17.1.199/24

Gre-ips 172.17.1.1/24

Gre-proxy 192.168.2.2/24

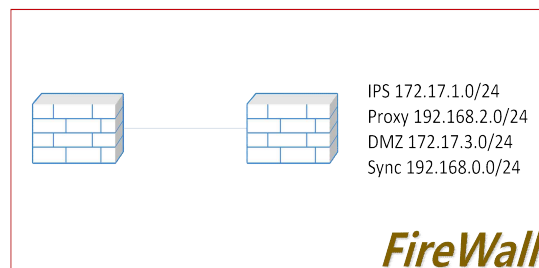
Gre-dmz 172.17.3.3/24

Gre-proxy 192.168.2.20/24

Gre-dmz 172.17.3.30/24

Gre-svr 172.17.10.5/24

Gre-svr 172.17.10.3/24

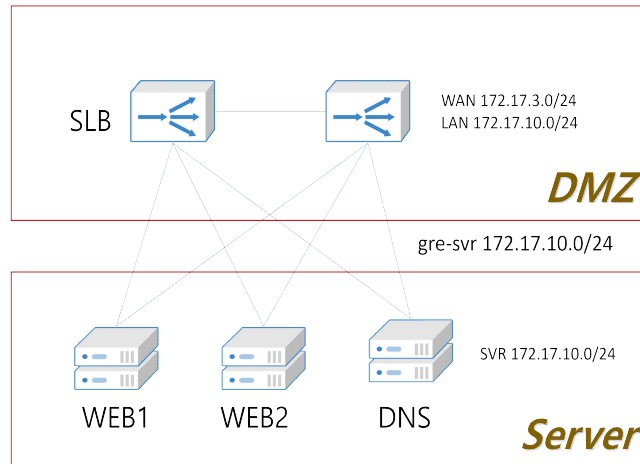


FW VM
BR1 10.201.0.2/16
Gre-ips 172.17.1.1/24
Gre-proxy 192.168.2.2/24
Gre-dmz 172.17.3.3/24

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

- SLB 구성도

gre-dmz 172.17.3.0/24



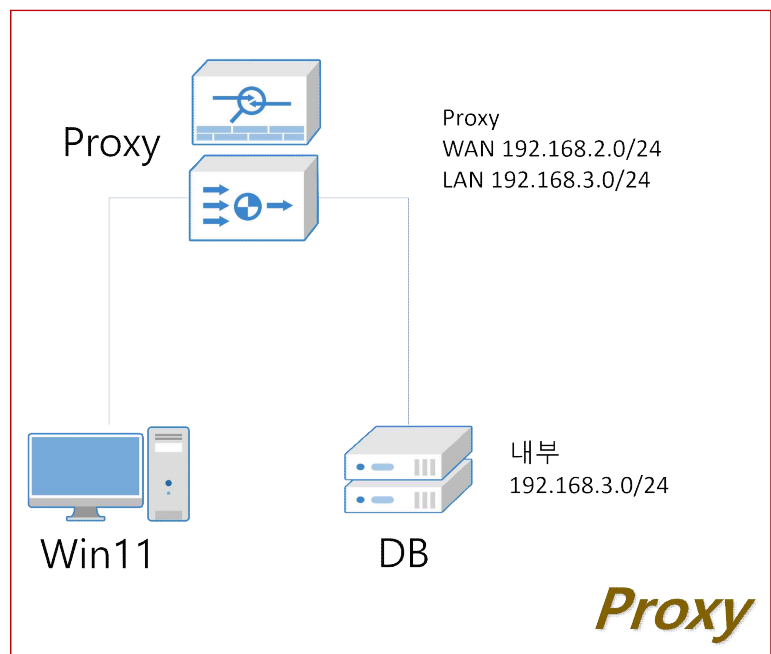
DMZ VM
BR1 10.201.0.10/16
Gre-dmz 172.17.3.30/24
Gre-svr 172.17.10.5/24

SVR VM
BR1 10.201.0.11/16
Gre-svr 172.17.10.3/24

- Proxy 구성도

gre-proxy 192.168.3.0/24

Proxy VM
BR1 10.201.0.3/16
Gre-proxy 192.168.2.20/24



프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

● 가상환경 구성 현황

※ 설치정보

Hypervisor OS	KVM
Server OS	AlmaLinux 9
Server	DB DNS WEB PHP
G/W	Vyos – 1.4.0
IPS / IDS	OPNsense - 24.7, SURIKATA
FireWall	OPNsense - 24.7
SLB	Vyos – 1.4.0
Proxy	OPNsense - 24.7, Squid
DB	MariaDB 10.5.22
LAN PC	Window11

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

- 네트워크 구성 현황

- IPS & IDS

구분 : IP

```
IPS VM
BR1 10.201.0.16/16
Gre-ips 172.17.1.15/24

IPS
WAN(iso)
172.17.4.100/24
LAN(gre)
172.17.1.100/24

Vynos1
WAN(br1)
10.201.0.101/24
Vip 10.201.0.100/24
LAN(iso)
172.17.4.11/24
Vip 172.17.4.1/24

Vynos2
WAN(br1)
10.201.0.102/24
Vip 10.201.0.100/24
LAN(iso)
172.17.4.12/24
Vip 172.17.4.1/24
```

내용 : IP 부여 정보

구분 : KVM -Almalinux 9

```
[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"
```

내용 : OVS_GRE 설정

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

구분 : Vynos1		
<pre> vynos@vynos# 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 </pre>		
<pre> vynos@vynos# ru show vrrp Name Interface VRID State Priority Last Transition ----- 1 eth0 1 MASTER 200 23h46m22s 2 eth1 2 MASTER 200 23h46m22s [edit] </pre>		
내용 : Interface 및 vrrp(마스터) 설정		

구분 : Vynos2		
<pre> vynos@vynos# 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 </pre>		
<pre> vynos@vynos# ru show vrrp Name Interface VRID State Priority Last Transition ----- 1 eth0 1 BACKUP 100 1h14m40s 2 eth1 2 BACKUP 100 1h14m40s [edit] </pre>		
내용 : Interface 및 vrrp(백업) 설정		

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

구분 : Vyos

```

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 {
        }
    }
}

```

```

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
            }
        }
    }
}

```

내용 : OSPF, NAT 설정

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

구분 : Vyos

```
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]
```

내용 : 라우팅 설정

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

- FireWall

구분 : IP	
	<div> FW VM BR1 10.201.0.2/16 Gre-ips 172.17.1.1/24 Gre-proxy 192.168.2.2/24 Gre-dmz 172.17.3.3/24 FW IPS(WAN) Fw-1 172.17.1.11/24 Fw-2 172.17.1.12/24 VIP 172.17.1.10/24 Proxy(LAN) Fw-1 192.168.2.11/24 Fw-2 192.168.2.12/24 VIP 192.168.2.10/24 DMZ(OPT) Fw-1 172.17.3.11/24 Fw-2 172.17.3.12/24 VIP 172.17.3.10/24 Sync(opt) Fw-1 192.168.0.1/24 Fw-2 192.168.0.2/24 </div>
내용 : IP 부여 정보	

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

구분 : Almalinux 9

```

[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"

```

내용 : OVS_GRE 설정

구분 : OPNsense

Interfaces: Virtual IPs: Status

Interface	VHID	Address	Status
LAN	1 (freq. 1/0)	192.168.2.10	MASTER
WAN	2 (freq. 1/0)	172.17.1.10	MASTER
OPT	3 (freq. 1/0)	172.17.3.10	MASTER

Showing 1 to 3 of 3 entries

내용 : FireWall VIP MASTER 설정

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

구분 : OPNsense

Interfaces: Virtual IPs: Status

Addresses

pfSync nodes

Search

CARP

7

Interface	VHID	Address	Status
LAN	1 (freq. 3/0)	192.168.2.10	▶ BACKUP
WAN	2 (freq. 3/0)	172.17.1.10	▶ BACKUP
OPT	3 (freq. 3/0)	172.17.3.10	▶ BACKUP

Showing 1 to 3 of 3 entries

내용 : FireWall VIP SLAVE 설정

구분 : OPNsense

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	▶ C ■
cron	Cron	▶ C ■
frr	FRRouting Daemon	▶ C ■
login	Users and Groups	▶ C
ntpd	Network Time Daemon	▶ C ■
pf	Packet Filter	▶ C
routing	System routing	▶ C
sysctl	System tunables	▶ C
syslog-ng	Syslog-ng Daemon	▶ C ■
unbound	Unbound DNS	▶ C ■
webui	Web GUI	▶ C ■

내용 : High Availablitystatus 화면 (이중화) 설정

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

구분 : OPNsense

1. OSPF

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

2.OSPF Neighbors

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

내용 : OSPF 설정 및 Neighbors

구분 : OPNsense

Routing: Diagnostics: General

IPv4 Routes

IPv6 Routes

Running Configuration

Code	Network	Administrative Dista...	Metric	Interface	Interface name	Via	Time
Q>*	0.0.0.0/0	110	10	vtnet2	WAN	172.17.1.100	00:56:38
Q>*	10.0.0.0/8	110	21	vtnet2	WAN	172.17.1.100	00:56:38
Q	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
Q>*	172.17.2.0/24	110	32	vtnet2	WAN	172.17.1.100	00:56:38
Q	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

내용 : OSPF & Staric 라우팅 테이블

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

- DMZ

구분 : IP	
	<pre> DMZ VM BR1 10.201.0.10/16 Gre-dmz 172.17.3.30/24 Gre-svr 172.17.10.5/24 DMZ SLB1 WAN(gre) 172.17.3.101/24 Vip 172.17.3.100 LAN(gre-srv) 172.17.10.11/24 Vip 172.17.10.10 SLB2 WAN(gre) 172.17.3.102/24 Vip 172.17.3.100 LAN(gre-srv) 172.17.10.12/24 Vip 172.17.10.10 SVR VM BR1 10.201.0.11/16 Gre-svr 172.17.10.3/24 SVR web1 172.17.10.101/24 web2 172.17.10.102/24 dns 172.17.10.150/24 </pre>
내용 : DMZ 및 Server 구간 IP 부여 정보	

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

구분 :KVM - Almalinux 9 - DMZ

```
[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"
```

내용 : OVS_GRE 설정

구분 :KVM - Almalinux 9 - SVR

```
[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"
```

내용 : OVS_GRE 설정 - DNS 서버

프로젝트 완료 보고서

프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

구분 : Vynos - SLB1

```

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 SLB1
vyos@SLB1# run sho vrrp

```

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

내용 : SLB1 inaterface 설정 및 VRRP(MASTER) 설정

구분 : Vynos - SLB2

```

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 {
  }
}

```

```

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

내용 : SLB2 inaterface 설정 및 VRRP(BACKUP) 설정

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

구분 : Vyos – SLB1,2

```
vyos@SLB1# sudo ip link set eth1 down
[edit]
vyos@SLB1# run show vrrp
```

Name	Interface	VRID	State	Priority	Last Transition
10	eth1	10	FAULT	105	7s
20	eth2	20	MASTER	105	1h16m58s

```
vyos@SLB2# run show vrrp
```

Name	Interface	VRID	State	Priority	Last Transition
10	eth1	10	BACKUP	100	1s
20	eth2	20	BACKUP	100	1h16m47s

```
[edit]
vyos@SLB2# run show vrrp
```

Name	Interface	VRID	State	Priority	Last Transition
10	eth1	10	MASTER	100	7s
20	eth2	20	BACKUP	100	1h17m4s

내용 :SLB1,2 VRRP Failover test

구분 : Vyos – SLB1,2

```
vyos@SLB1# sudo ip link set eth1 up
[edit]
vyos@SLB1# run show vrrp
```

Name	Interface	VRID	State	Priority	Last Transition
10	eth1	10	MASTER	105	3s
20	eth2	20	MASTER	105	1h17m29s

```
vyos@SLB2# run show vrrp
```

Name	Interface	VRID	State	Priority	Last Transition
10	eth1	10	BACKUP	100	6s
20	eth2	20	BACKUP	100	1h17m35s

내용 :SLB1,2 VRRP Failback test

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

구분 : Vynos - SLB1
 <pre> 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 } } } </pre>
내용 : SLB1 OSPF 설정

구분 : Vynos - SLB2
 <pre> 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 } } } </pre>
내용 : SLB2 OSPF 설정

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

구분 : Vyos - SLB1

```

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

```

내용 : SLB1 라우팅 테이블

구분 : Vyos - SLB2

```

root@localhost:~ — virsh console SLB2
vyos@SLB2# run 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 172.17.3.11, eth1, weight 1, 00:19:14
O>* 10.0.0.0/8 [110/22] via 172.17.3.11, eth1, weight 1, 00:19:15
O>* 172.17.1.0/24 [110/11] via 172.17.3.11, eth1, weight 1, 00:19:25
O>* 172.17.2.0/24 [110/33] via 172.17.3.11, eth1, weight 1, 00:19:15
O  172.17.3.0/24 [110/1] is directly connected, eth1, weight 1, 00:21:15
C>* 172.17.3.0/24 is directly connected, eth1, 01:10:13
O>* 172.17.4.0/24 [110/21] via 172.17.3.11, eth1, weight 1, 00:19:15
O  172.17.10.0/24 [110/1] is directly connected, eth2, weight 1, 01:10:10
C>* 172.17.10.0/24 is directly connected, eth2, 01:10:12
O>* 172.17.100.0/24 [110/43] via 172.17.3.11, eth1, weight 1, 00:19:15
O>* 172.17.200.0/24 [110/43] via 172.17.3.11, eth1, weight 1, 00:19:15
O>* 192.168.50.0/24 [110/20] via 172.17.3.11, eth1, weight 1, 00:19:14
O>* 192.168.51.0/24 [110/53] via 172.17.3.11, eth1, weight 1, 00:19:15

```

내용 : SLB2 라우팅 테이블

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

- Proxy

구분 : IP
<div> Proxy VM BR1 10.201.0.3/16 Gre-proxy 192.168.2.20/24 Proxy WAN(gre) 192.168.2.101/24 LAN(iso) 192.168.3.201/24 Win11 192.168.3.202/24 DB 192.168.3.203/24 </div>
내용 : IP 부여 정보

구분 : KVM - Almalinux9
<pre> 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" </pre> <pre> 1: gre-proxy: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000 link/ether 1e:50:ce:14:e8:4c brd ff:ff:ff:ff:ff:ff inet 192.168.2.20/24 scope global gre-proxy valid_lft forever preferred_lft forever </pre>
내용 : OVS_GRE 설정

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

구분 : OPNsense - Proxy

Routing: STATIC

General Routes

Q Search

↺ 7 ↻

⌵

<input type="checkbox"/> Enabled	Network	Gateway	Interface	Commands
<input type="checkbox"/> <input checked="" type="checkbox"/>	0.0.0.0/0	192.168.2.10	WAN	<div>✎ 📄 🗑</div> <div>+ 🗑</div>

1

Showing 1 to 1 of 1 entries

Firewall: NAT: Outbound

Mode

☐ Automatic outbound NAT rule generation
(no manual rules can be used)

☐ Hybrid outbound NAT rule generation
(automatically generated rules are applied after manual rules)

☒ Manual outbound NAT rule generation
(no automatic rules are being generated)

☐ 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 checked="" type="checkbox"/>	WAN	any	*	*	*	WAN address	*	NO		↶	✎	🗑	🔍

내용 : Static 설정 및 NAT 설정

구분 : opnsense - Proxy

```

Hello, this is FRRouting (version 8.5.6).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

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

S    0.0.0.0/0 [1/0] via 192.168.2.10, vtnet0, weight 1, 08:04:57
OPNsense.localdomain#

```

내용 : Proxy 라우팅 설정

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

- 상세 구축 및 구성 내용
나) FireWall 구성 현황

OPNsense – FireWall

1. WAN

Firewall: Rules: WAN

Select category

Inspect

	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

내용 : WAN 인터페이스의 80, 53, 443 포트를 제외한 접속 차단

OPNsense – FireWall

2. OPT

Firewall: Rules: OPT

Select category

Inspect

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
Automatically generated rules									14
<input type="checkbox"/>	IPv4 TCP	*	*	*	80 (HTTP)	*	*		<input type="checkbox"/> <input type="pencil"/> <input type="trash"/> <input type="refresh"/>
<input type="checkbox"/>	IPv4 TCP	*	*	*	443 (HTTPS)	*	*		<input type="checkbox"/> <input type="pencil"/> <input type="trash"/> <input type="refresh"/>
<input type="checkbox"/>	IPv4 UDP	*	*	*	53 (DNS)	*	*		<input type="checkbox"/> <input type="pencil"/> <input type="trash"/> <input type="refresh"/>
<input type="checkbox"/>	IPv4 ICMP	172.17.10.0/24	*	192.168.3.0/24	*	*	*		<input type="checkbox"/> <input type="pencil"/> <input type="trash"/> <input type="refresh"/>
<input type="checkbox"/>	IPv4 TCP	172.17.10.0/24	*	192.168.3.0/24	3306	*	*		<input type="checkbox"/> <input type="pencil"/> <input type="trash"/> <input type="refresh"/>
<input type="checkbox"/>	IPv4 *	OPT net	*	OPT net	*	*	*		<input type="checkbox"/> <input type="pencil"/> <input type="trash"/> <input type="refresh"/>

내용 : OPT 인터페이스의 80, 53, 443, 3306 포트를 제외한 접속 차단

OPNsense – FireWall

3. LAN

Firewall: Rules: LAN

Select category



Inspect

	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)	*	*		<div> <div></div> <div></div> <div></div> <div></div> </div>
<input type="checkbox"/>	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	*		<div> <div></div> <div></div> <div></div> <div></div> </div>
<input type="checkbox"/>	IPv4 UDP	LAN net	*	*	53 (DNS)	*	*		<div> <div></div> <div></div> <div></div> <div></div> </div>
<input type="checkbox"/>	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	*		<div> <div></div> <div></div> <div></div> <div></div> </div>
<input type="checkbox"/>	IPv4 *	LAN net	*	LAN net	*	*	*		<div> <div></div> <div></div> <div></div> <div></div> </div>


내용 : LAN 인터페이스의 80, 53, 443, 3306 포트를 제외한 접속 차단

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

다) SLB 구성 현황

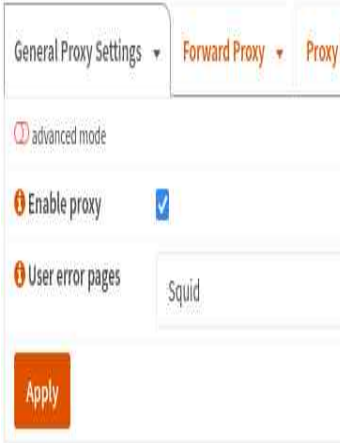
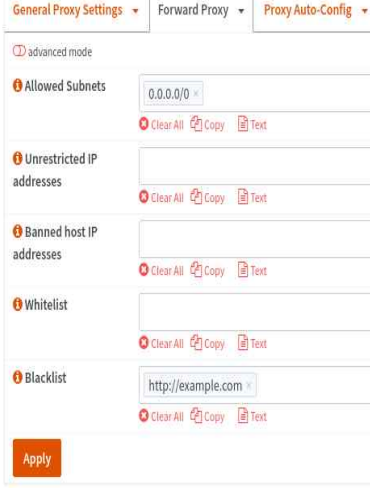
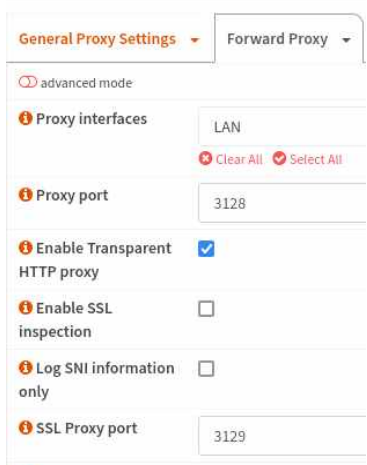
Load-balancing : SLB1	Load-balancing : SLB2
 root@localhost:~ — virsh console SL <pre> load-balancing { reverse-proxy { backend web-backend { balance round-robin mode http server web1 { address 172.17.10.101 port 80 } server web1-https { address 172.17.10.101 port 443 } server web2 { address 172.17.10.102 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 } } </pre>	 root@localhost:~ — virsh console SL <pre> 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 } } </pre>
내용 : SLB1 의 Load-balancing 설정	

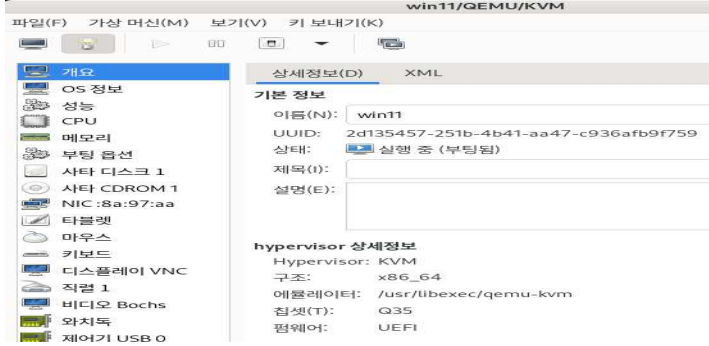
프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

DNS 서버 설정	
 <pre> \$TTL 3H @ IN SOA nonblindsite.com. nonblindsite.com. (0 ; serial 1D ; refresh 1H ; retry 1W ; expire 3H ; minimum) @ IN NS 172.17.10.150 www IN A 172.17.10.101 www IN A 172.17.10.102 www IN A 172.17.10.10 IN AAAA ::1 </pre>	
내용 : DNS 서버 구성	

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

라) Proxy 구성 현황

OPNsense - Proxy		WAN IP : 192.168.2.101 LAN IP : 192.168.3.201
		
<p>내용 :</p> <ul style="list-style-type: none"> - HTTP Proxy 기능 활성화 - http://example.com 사이트 블랙리스트 등록 		

내부 네트워크 PC : Win11	IP : 192.168.3.202/24
	
<p>내용 :</p> <ul style="list-style-type: none"> - Win11을 활용한 내부 pc 구성 - CPU(2Core) / Memory(10GB) / Disk (Usable :60GB(KVM할당)) 	

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

Server Name : DB	IP : 192.168.3.203/24
------------------	-----------------------



내용 :

- Almalinux9를 기반 Mariadb 서버 구축
- CPU(2Core) / Memory(4GB) / Disk (Usable : 20GB(KVM 할당))

DB 구성

```

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 |
+-----+

```

내용 : DB 생성 및 권한 부여

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승현	작성일 : 25.02.04

● 구축 결과

가) IPS & IDS 구성 현황

- IP 통신 차단

OPNsense – IPS & IDS

1. IP 통신 차단

Search

2025/02/12 0:30

7

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	

내용 : SURIKATA를 통한 10.10.10.16 IP 차단 로그

IP 통신 차단 결과
<pre> 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 </pre>
내용 : 10.10.10.16 IP 차단 결과

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

- Land Attack

OPNsense – IPS & IDS

2. Land Attack 공격 탐지

Search

↺

🗑

2025/02/11 7:28

▼

7▼

☰▼

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

내용 : SURIKATA를 통한 Land Attack 공격 탐지 로그

Land Attack 공격 탐지 결과
<pre> (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 </pre>
내용 : Kali를 통한 land attack 공격 탐지 결과

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

-ICMP Ping flood

OPNsense – IPS & IDS

3.ICMP Ping Flood 차단

Search

↺

🗑

2025/02/12 1:27

▼

7

⌵

timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	🔗
025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	🔗
025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	🔗
025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	🔗
025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	🔗
025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	🔗
025-02-12T01:27:53.558942+0000	1000001	blocked	wan	172.17.4.200	0	172.17.10.10	0	ICMP Ping Flood detected	🔗

⏪

1

2

⏩


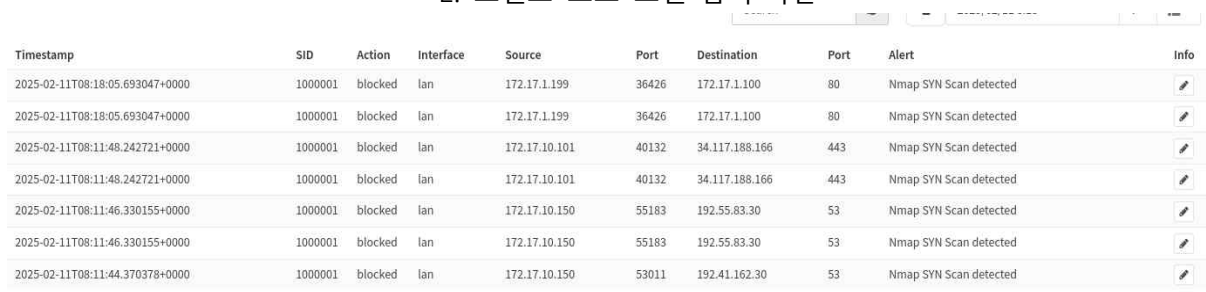
Showing 1 to

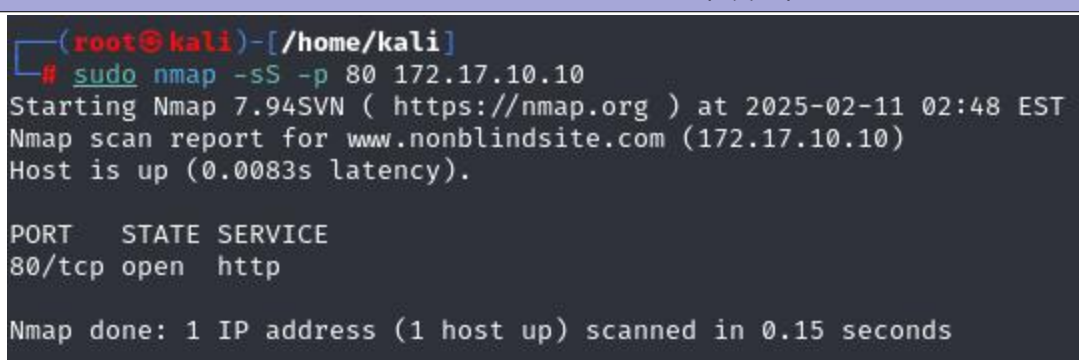
내용 : SURIKATA를 통한 ICMP Ping Flood 차단 로그

ICMP Ping Flood 차단
<pre> (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 </pre>
내용 : Kali를 통한 ICMP Ping Flood 차단 결과

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

- 스텔스 포트 스캔탐지

OPNsense – IPS & IDS		4.스텔스 포트 스캔 탐지 및 차단
<p>1. 스텔스 포트 스캔 탐지</p> 		
<p>2. 스텔스 포트 스캔 탐지-차단</p> 		
내용 : SURIKATA를 통한 스텔스 포트 스캔 탐지 및 차단로그		

스텔스 포트 스캔 탐지 및 차단

내용 : Kali를 통한 스텔스 포트 스캔 탐지 및 차단 결과

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

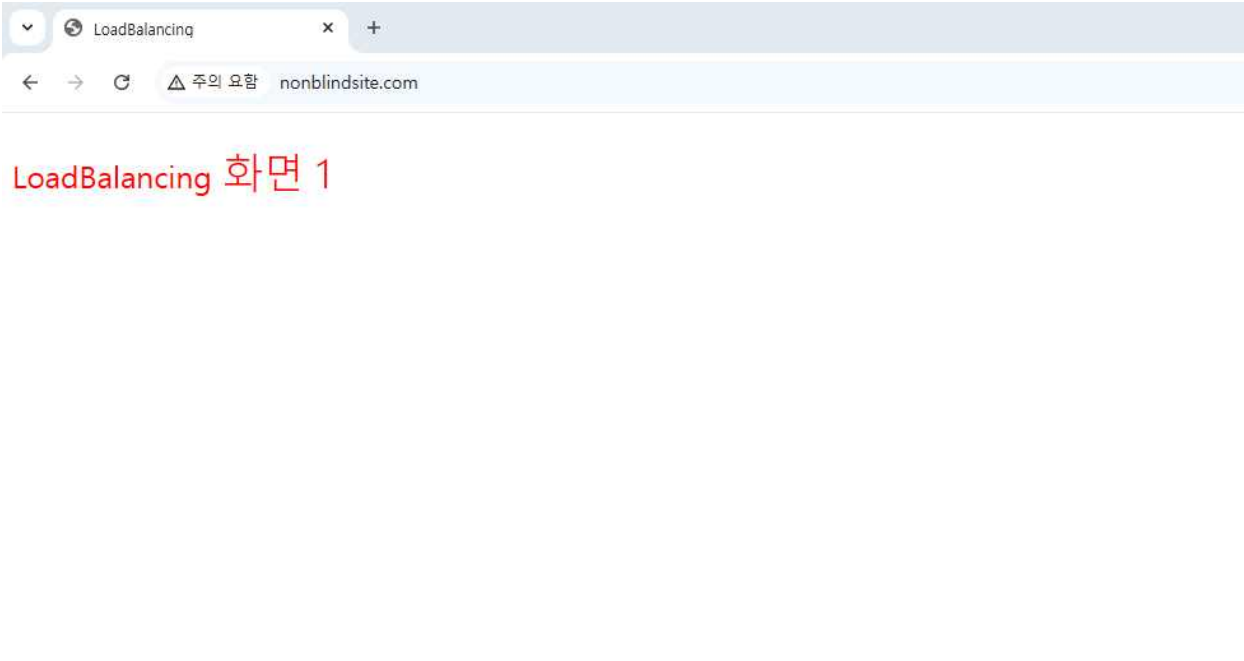
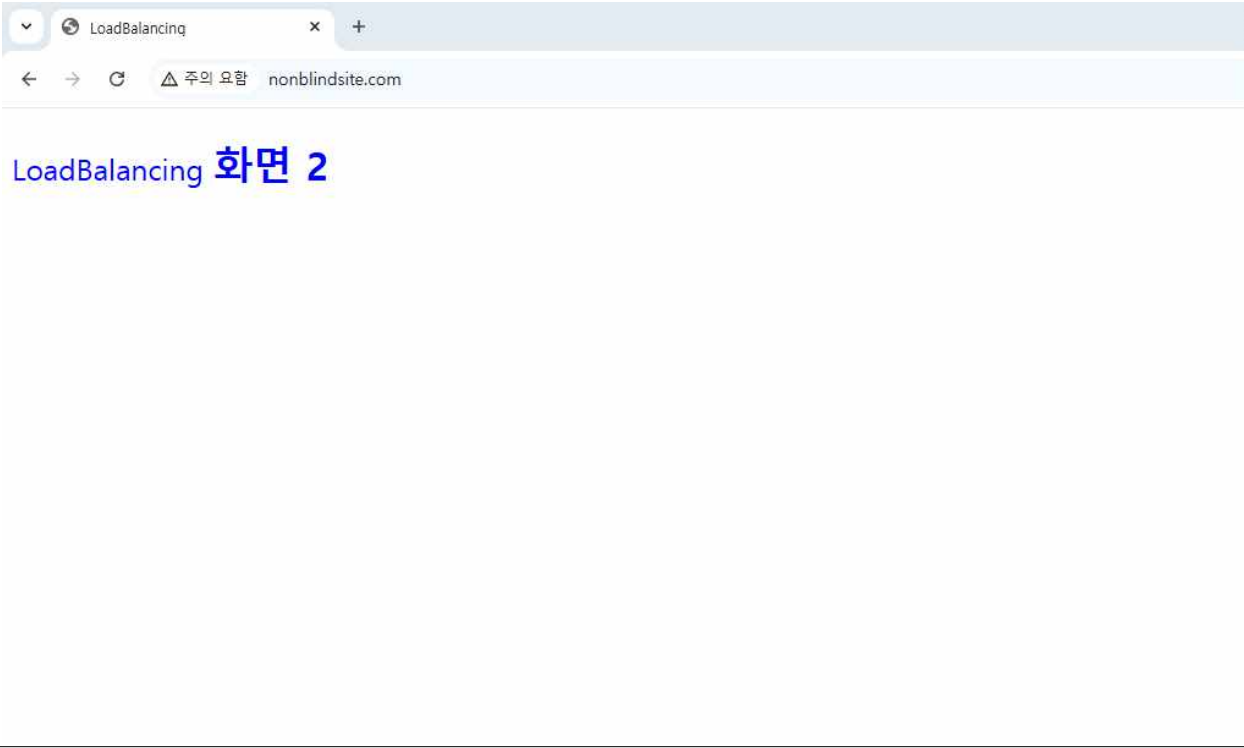
나) SLB 구축 결과

내부구간 Win11을 통한 www.nonblindsite.com 접속테스트 (SLB)



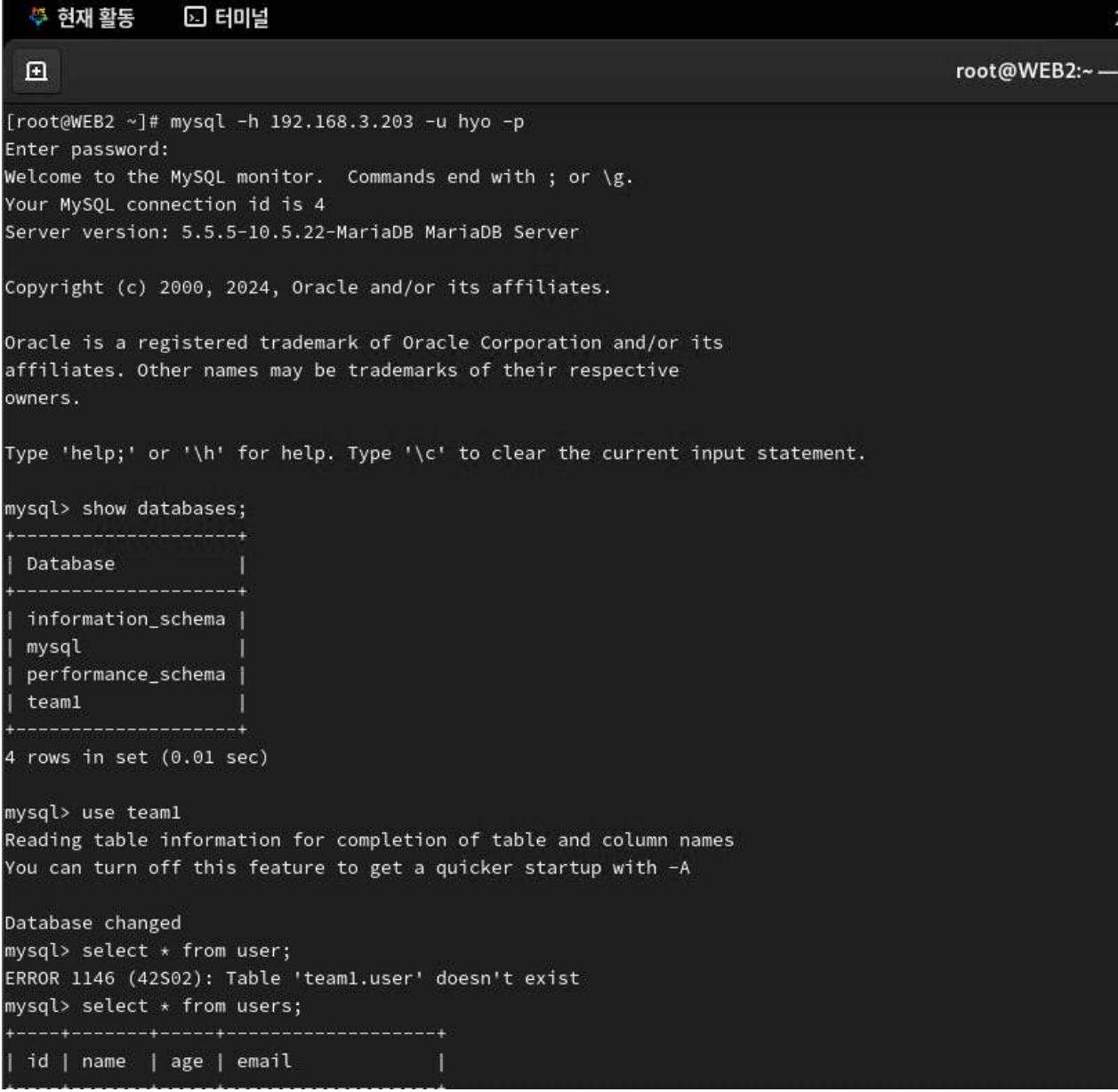
내용 : SLB 설정을 완료하여, www.nonblindsite.com 을 방문할시 www.nbs1.com 과 www.nbs2.com 이 번갈아가며 접속

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

외부구간 Host PC 통한 www.nonblindsite.com 접속테스트 (SLB)	
	
	
<p>내용 : SLB 설정을 완료하여, www.nonblindsite.com 을 방문할시 www.nbs1.com 과 www.nbs2.com 이 번갈아가며 접속</p>	

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

다) 내부 구간 - DMZ 구간 통신 구축 결과

DMZ 구간 서버 - LAN 구간 DB 서버 접속 확인
 <pre> 현재 활동 터미널 root@WEB2:~ — [root@WEB2 ~]# mysql -h 192.168.3.203 -u hyo -p Enter password: Welcome to the MySQL monitor. Commands end with ; or \g. Your MySQL connection id is 4 Server version: 5.5.5-10.5.22-MariaDB MariaDB Server Copyright (c) 2000, 2024, Oracle and/or its affiliates. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Type 'help;' or '\h' for help. Type '\c' to clear the current input statement. mysql> show databases; +-----+ Database +-----+ information_schema mysql performance_schema team1 +-----+ 4 rows in set (0.01 sec) mysql> use team1 Reading table information for completion of table and column names You can turn off this feature to get a quicker startup with -A Database changed mysql> select * from user; ERROR 1146 (42S02): Table 'team1.user' doesn't exist mysql> select * from users; +----+-----+-----+-----+ id name age email +----+-----+-----+-----+ </pre>
내용 : CLI 통한 DB 접속 및 제어

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

phpMyAdmin db 접속

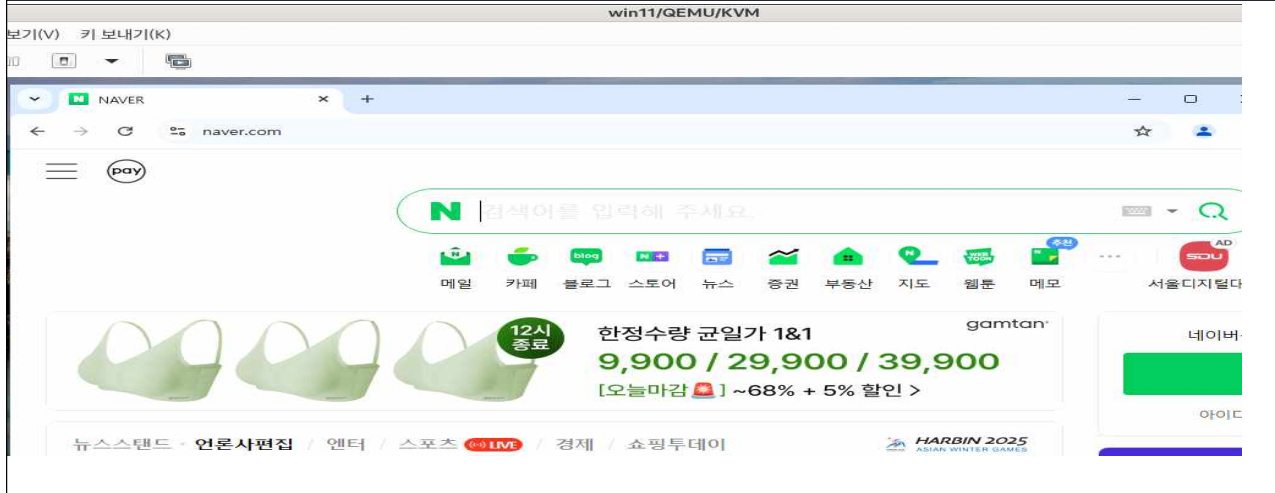


내용 : WEB 연결 후 phpMyAdmin을 통한 DB 접속 및 제어

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04


라) Proxy 구축 결과

Win11을 통한 NAVER접속 테스트

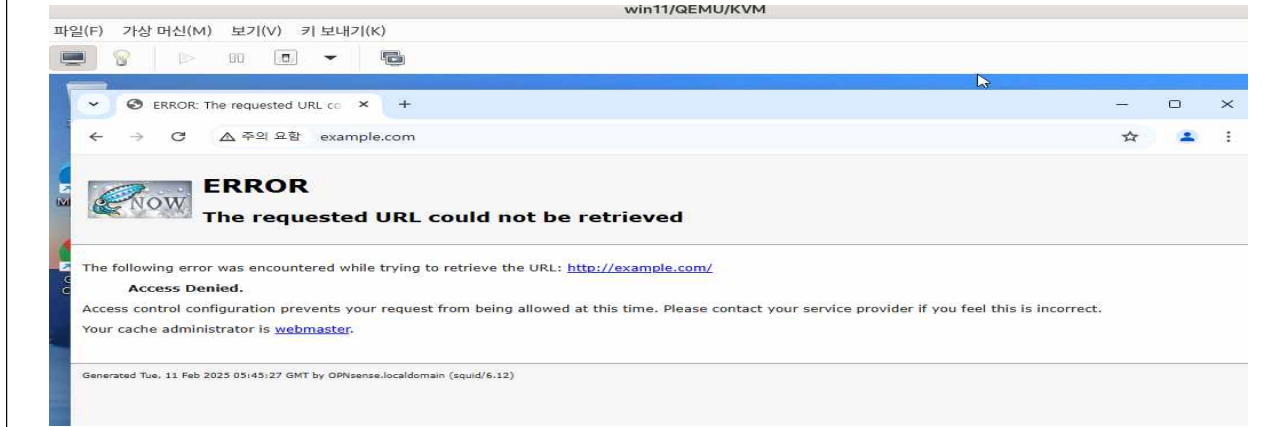


내용 : 내부 네트워크의 외부 접속 테스트

투명 Proxy를 통한 <http://example.com> 접속 테스트



Proxy 설정 후



내용 : 투명 프록시 특정 사이트 접속 차단 테스트

프로젝트 완료 보고서		
프로젝트 주제	CCTV 네트워크 회사의 KVM 기반 백본망 및 보안 인프라 구축	
단계 : 프로젝트 완료	작성자 : 지승헌	작성일 : 25.02.04

4. 개별 후기

● 권효중 후기

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.

● 이효운 후기

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 후기

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.

● 지승헌 후기

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.