

2026년 지방기능경기대회 과제

직 종 명	IT네트워크시스템	과 제 명	Linux Environments	과제번호	제1과제
경기시간	4시간	비 번 호		심사위원 확 인	(인)

1. 과제 소개

가. 과제 개요

해당 과제는 과년도 국제기능올림픽 대회 과제를 기반으로 디자인된 과제입니다. 모든 서비스는 Dual Stack(IPv4 및 IPv6)을 지원해야 하며 과제 요구사항에 따라 네트워크 서비스, 인증 시스템, 디렉토리 서비스, 메일 서비스 및 웹 서비스를 적절히 구축합니다. 서비스 구현 시 특정 패키지가 지정되었을 경우 반드시 해당 패키지를 사용해야 합니다.

나. 소프트웨어 요구사항

- 1) VMWare Workstation 최신버전
- 2) Debian Linux 12.8

다. 지급 재료

- 1) code_1.97.2-1739406807_amd64.deb

라. 주의 사항

- 1) 리눅스 관리자 계정은 "root"이며 기본 사용자 계정은 "sysop"입니다.
- 2) 시스템 구축 진행 시 암호가 필요할 경우 "Skill39**"을 기본값으로 사용합니다.
- 3) 특별하게 지정되지 않은 옵션 또는 설정은 시스템이 추천하는 기본값을 사용합니다.
- 4) 리눅스 시스템에 설치되는 모든 패키지의 무결성이 훼손되지 않도록 주의합니다.
- 5) 정해진 USB장치 이외의 저장장치의 반입을 금지합니다.
- 6) 경기 시작 전 휴대폰 등과 같은 스마트기기는 심사위원(또는 관리 위원)에게 보관하도록 합니다.
- 7) 경기 종료 후 임의로 설정을 변경하거나 서비스를 재시작할 수 없으며 채점 시 모든 서비스가 정상적으로 동작되어야 합니다.

2. 과제 요구사항

A. fw.worldskills.org

가. 네트워킹 서비스

- 1) 이 장치는 라우터, 방화벽 및 투명 프록시 서버로 동작합니다.
- 2) IPv4 및 IPv6 트래픽을 포워딩 할 수 있도록 구성합니다.

나. 방화벽 서비스

- 1) nftables 방화벽 정책을 구성합니다.
- 2) IPv4 정책
 - a) 내부 네트워크 및 DMZ 네트워크에서 외부 네트워크로 향하는 트래픽은 허용되어야 합니다.
 - b) 내부 네트워크에서 DMZ 네트워크로 향하는 트래픽은 허용되어야 합니다.
 - c) 외부 네트워크에서 FW 디바이스의 VPN(51820/udp) 서비스에 접근할 수 있도록 합니다.
 - d) mail 디바이스는 int-srv 디바이스의 LDAP(389/tcp) 서비스에 접근할 수 있도록 합니다.
 - e) VPN에 연결된 디바이스는 내부 네트워크 및 DMZ 네트워크로 접근할 수 있도록 합니다.
 - f) 명시된 트래픽 외에 모든 트래픽을 기본적으로 차단합니다.
 - g) 외부 네트워크로 향하는 모든 트래픽은 모두 Masquerade NAT 처리되어 주소 변환되어야 합니다.
 - h) 외부 네트워크 인터페이스로 유입되는 HTTP(80/tcp), HTTPS(443/tcp) 및 DNS(53/udp, 53/tcp) 트래픽은 DMZ의 고가용성 디바이스로 포워딩 되어야 합니다.
- 3) IPv6 정책
 - a) 내부 네트워크 및 DMZ 네트워크에서 외부 네트워크로 향하는 트래픽은 허용되어야 합니다.
 - b) 내부 네트워크에서 DMZ 네트워크로 향하는 트래픽은 허용되어야 합니다.
 - c) 외부 네트워크에서 DMZ 네트워크의 고가용성 디바이스로 향하는 HTTP(80/tcp), HTTPS(443/tcp) 및 DNS(53/udp, 53/tcp) 트래픽은 허용되어야 합니다.
 - d) VPN에 연결된 디바이스는 내부 네트워크 및 DMZ 네트워크로 접근할 수 있도록 합니다.
 - e) 명시된 트래픽 외에 모든 트래픽을 기본적으로 차단합니다.

다. VPN 서비스

- 1) 외부 네트워크의 디바이스가 내부 네트워크 및 DMZ 네트워크로 보안 연결을 할 수 있도록 WireGuard VPN 서비스를 구성합니다.
- 2) 부록을 참조하여 VPN 터널 네트워크 주소를 설정합니다.
- 3) VPN 연결 후 클라이언트의 모든 트래픽이 VPN 터널을 통해 전달되도록 구성합니다.
- 4) VPN 연결 후 도메인 정보 조회 시 내부 네트워크의 DNS 서버를 사용하도록 합니다.
- 5) WireGuard 서비스는 wg-quick 시스템 데몬으로 관리되어야 하며 VPN 설정 파일은 "/etc/wireguard/wg0.conf"에 배치되어야 합니다.

라. 투명 프록시 서비스

- 1) Squid 투명 프록시 서비스를 구성합니다. 투명 프록시 구성 시 서비스 포트 (tcp/8080)를 사용하도록 합니다.
- 2) 내부 네트워크 및 VPN 네트워크에서 발생한 HTTP(tcp/80) 트래픽이 투명 프록시 서버에 의해 가로채지도록 구성합니다.
- 3) 프록시 처리된 트래픽의 헤더에 다음 내용이 추가되어야 합니다.
x-secured-by: worldskills-prx

B. int-srv.int.worldskills.org

가. LDAP 서비스

- 1) LDAP 디렉토리 서비스를 설치하고 "int.worldskills.org" 도메인에 대한 데이터베이스를 추가합니다.
- 2) LDAP 서버는 사용자가 메일 서버에 로그인할 때 인증을 위해 사용됩니다.
- 3) 아래 표를 참조하여 LDAP 엔트리를 구성하도록 합니다.

Username	OU	UID	GID	mail
ws-user01	Employees	2001	2001	ws-user01@worldskills.org
ws-user02		2002	2002	ws-user02@worldskills.org

나. Samba 서비스

- 1) Samba 파일 서비스를 구성합니다.
- 2) Samba 서비스는 독립적인 사용자 데이터베이스로 운영되어야 하며 인증을 위한 "ws-user" 사용자 계정을 추가합니다.
- 3) 공유 서비스를 구성합니다.
 - a) "public" 공유는 게스트를 포함한 모든 사용자에게 읽기 권한을 부여하며 로그인한 사용자만 파일을 작성할 수 있습니다.
 - b) "internal" 공유는 인증된 사용자만 읽기 및 쓰기 권한을 부여하며 게스트 사용자는 이 공유에 접근할 수 없습니다.

다. 인증기관 서비스

- 1) 루트 인증기관을 구성합니다.
 - a) 인증기관 저장소는 "/etc/ssl/ws-RootCA" 입니다.
 - b) 인증기관의 Common Name은 "worldskills-RootCA" 로 구성하며 이 외의 인증서 속성 값은 임의로 설정합니다.
 - c) 루트 인증기관에서 하위 인증기관 인증서를 발급합니다.
- 2) 하위 인증기관을 구성합니다.
 - a) 인증기관 저장소는 "/etc/ssl/ws-SubCA" 입니다.
 - b) 인증기관의 Common Name은 "worldskills-SubCA" 로 구성하며 이 외의 인증서 속성 값은 임의로 설정합니다.
 - c) 하위 인증기관에서 서비스 인증서를 발급합니다.
- 3) OpenSSH 인증기관을 구성합니다.
 - a) 인증기관 저장소는 "/etc/ssl/ssh-CA"입니다.
 - b) SSH 서비스용 인증서를 발급합니다.

라. DNS 서비스

- 1) BIND9 DNS 서비스를 구성합니다.
- 2) "int.worldskills.org" 도메인에 대한 정방향 도메인 존을 구성합니다.
내부 네트워크 디바이스의 FQDN 대한 정방향 레코드를 추가합니다.
- 3) 내부 네트워크의 IP 주소에 대한 역방향 도메인 존을 구성합니다.
내부 네트워크 디바이스의 FQDN 대한 역방향 레코드를 추가합니다.
- 4) DMZ 네트워크의 DNS 서버로부터 "worldskills.org" 도메인 정보를 동기화합니다.
- 5) DMZ 네트워크의 DNS 서버로부터 역방향 도메인 정보를 동기화합니다.
- 6) 내부 네트워크 및 VPN 네트워크의 장치가 도메인 쿼리를 할 수 있도록 구성합니다.

C. mail.worldskills.org

가. 메일 서비스

- 1) Postfix 및 Dovecot을 활용하여 "worldskills.org" 도메인에 대한 메일 서비스를 구성합니다.
- 2) LDAP 사용자를 이용하여 메일 서비스를 사용할 수 있도록 구성합니다.
LDAP 데이터베이스의 uid 속성 값으로 메일 시스템에 로그인 할 수 있어야 하며 mail 속성 값을 메일 주소로 사용합니다.
- 3) IMAP(tcp/143) 및 IMAPS(tcp/993) 를 통해 사용자가 자신의 메일함에 접근할 수 있어야 합니다.
- 4) SMTP(tcp/25, 587) 및 SMTPS(tcp/465) 를 통해 사용자가 메일을 송신할 수 있어야 합니다.
- 5) 서버와 클라이언트 간 모든 통신은 TLS 보안이 적용되어야 하며 보안 구성을 위해 인증 기관에서 발급 받은 인증서를 사용하도록 합니다.
- 6) 메일 자동 응답 서비스를 구성합니다.
 - a) "echo@worldskills.org" 메일 주소로 메일이 송신될 경우 자동으로 응답을 전송해야 합니다.
 - b) 자동 응답 시 메일 제목은 "Re: {송신된 메일 제목}" 형식이며 내용은 "worldskills mail service"로 메일이 응답 되어야 합니다.

나. 원격 관리 서비스

- 1) SSH 기반 원격 접속을 구성합니다.
- 2) 인증 기관으로부터 발급받은 인증서를 활용해 중앙화된 공개키 기반 인증을 지원하도록 구성합니다.
- 3) int-srv 디바이스에서 해당 장치의 root 계정으로 원격 접근 시 인증서 기반 인증을 수행하도록 구성합니다.

다. 백업 서비스

- 1) 백업 디스크를 디바이스에 추가한 후 "/backup" 위치에 디스크를 마운트 합니다. 해당 디스크는 서버 부팅 시 자동으로 마운트 되어야 합니다.
- 2) 서버 구동에 문제가 발생하는 상황을 대비하여 메일 시스템 데이터 백업을 구성합니다.
 - a) "mailbox", "postfix" 및 "dovecot" 디렉토리를 백업 위치 하위에 생성하고 메일박스 데이터 및 메일 서비스 구성 파일을 백업 디스크에 자동으로 백업하는 스크립트를 작성합니다.
 - b) 서버의 완전한 손실이 발생하더라도 해당 백업 데이터를 이용해 메일 서버를 복구할 수 있어야 합니다.
 - c) 백업 스크립트 파일을 "/opt/backup.sh"로 저장하십시오. 해당 스크립트를 활용하여 매분 데이터 백업을 수행합니다.

라. NTP 서비스

- 1) chrony를 활용하여 구성합니다.
- 2) NTP 서버는 prx로 지정합니다.
- 3) 보안 강화를 위해 NTP 서비스에 MD5 키 기반 인증을 구성합니다.
 - a) 키 번호는 9번을 사용하며 Password는 Skill39**를 사용합니다.

마. NFS

- 1) CLIENT와 파일을 공유 할 수 있도록 설정합니다.
- 2) 파일의 경로는 /root/shares이며 int-srv는 해당 파일에서 읽고 쓸 수 있도록 구성합니다.
- 3) 서버와 클라이언트 간 NFS 통신은 SSL/TLS를 이용한 Stunnel로 보호하도록 구성합니다.
- 4) Stunnel 포트의 경우, 52000번을 사용하여 client와 통신할 수 있도록 구성합니다.

바. RAID

- 1) 30GB SCSI 디스크를 4개 추가하며 RAID 5를 사용하여 구성합니다.
- 2) 4개의 디스크를 하나의 RAID 장치로 생성합니다.
- 3) 모든 SCSI 디스크의 GPT 파티션 테이블로 초기화하며 1개의 파티션을 생성합니다.
- 4) 해당 파티션은 ext4 파일 시스템을 생성하며 /mnt/raid에 마운트 하도록 구성합니다.
- 5) 해당 디바이스 부팅 시 자동으로 위에 제시된 경로에 마운트 되어야 합니다.

D. prx01.worldskills.org / prx02.worldskills.org

가. 고가용성 서비스

- 1) prx01 및 prx02 디바이스가 고가용성이 보장되는 리버스 프록시 및 DNS 서버, NTP 서버로 동작하도록 구성합니다.
- 2) 각 디바이스의 서비스에 고가용성 가상 주소로 접근 가능하도록 구성합니다.
 - a) IPv4 : 10.1.20.20/24
 - b) IPv6 : 2001:db8:1001:20::20/64

나. 리버스 프록시 서비스

- 1) HTTP 및 HTTPS 서비스에 대한 리버스 프록시 서비스를 구성합니다.
해당 서버는 TLS Termination을 수행해야 합니다.
- 2) HTTP 요청은 HTTPS로 리디렉션되어야 합니다.
- 3) 하나의 웹 서버가 다운될 경우, 요청이 다른 웹 서버로 전달되어야 합니다.

- 4) 프록시 서버가 응답에 다음 헤더를 추가하도록 합니다.
via-proxy: {웹 서비스 호스트네임}
- 5) 하위 인증기관으로부터 TLS 서비스를 위한 인증서를 발급 받습니다.

다. DNS 서비스

- 1) BIND9 DNS 서비스를 구성합니다. prx01 디바이스를 주 도메인 서버로 구성하고 prx02 디바이스는 보조 도메인 서버로 구성합니다.
- 2) "worldskills.org" 도메인에 대한 정방향 도메인 존을 구성합니다.
 - a) DMZ 네트워크 디바이스의 FQDN 대한 정방향 레코드를 추가합니다.
 - b) 고가용성 가상 주소에 대한 도메인 서비스 레코드(ns) 및 웹 서비스 레코드(www)를 추가합니다.
 - c) mail 디바이스의 메일 서비스에 대한 메일 교환 레코드를 추가합니다.
- 3) DMZ 네트워크의 IP 주소에 대한 역방향 도메인 존을 구성합니다.
 - a) DMZ 네트워크 디바이스의 FQDN 대한 역방향 레코드를 추가합니다.
 - b) 서비스에 대한 역방향 레코드를 추가합니다.
- 4) 해당 서버는 권한 있는 도메인 존에 대해서만 응답하도록 구성합니다.

라. NTP 서비스

- 1) Chrony를 활용하여 NTP 서비스를 구성합니다.
- 2) 10.1.20.0/24 범위에 있는 모든 디바이스는 NTP 서버로부터 시간 서비스를 제공받아야 합니다.
- 3) 10.1.20.0/24 범위 외에 있는 모든 디바이스의 경우 NTP 서비스 연결 시도 시 차단되어야 합니다.
- 4) 보안 강화를 위해 NTP서비스에 MD5 키 기반 인증을 구성합니다.
 - a) 키 번호는 9번을 사용하며 Password는 Skill39**를 사용합니다.
- 5) prx01이 다운 시 prx02가 NTP 서버 역할을 수행합니다.
- 6) 테스트를 위해 int-srv 및 10.1.20.0/24 디바이스에 chrony 설정을 구성합니다.

E. web01.worldskills.org / web02.worldskills.org

가. 웹 서비스

- 1) web01 및 web02 디바이스에 "www.worldskills.org" HTTP 웹사이트를 호스팅 합니다.
- 2) 웹 서비스 접근 시 "worldskills web service" 콘텐츠가 출력되어야 합니다.
- 3) 웹 서비스의 "/whoami" 경로 접근 시 서버 호스트 명이 반환되도록 합니다.
- 4) 해당 서버에서 404 Not Found 오류를 반환해야 하는 경우
"Contents Unavailable" 콘텐츠가 반환되도록 합니다.

나. 원격 관리 서비스

- 1) SSH 기반 원격 접속을 구성합니다.
- 2) 인증 기관으로부터 발급받은 인증서를 활용해 중앙화된 공개키 기반 인증을 지원하도록 구성합니다.
- 3) int-srv 디바이스에서 해당 장치의 root 계정으로 원격 접근 시 인증서 기반 인증을 수행하도록 구성합니다.

다. 자동화 서비스

- 1) int-srv 디바이스에서 web01 및 web02 디바이스의 웹 서비스를 자동화 기반으로 제어할 수 있도록 구성합니다.
- 2) 웹 서비스 요구사항을 준수하는 웹 서비스를 배포 및 제거할 수 있도록 Ansible 자동화 서비스를 구성합니다.
 - a) 웹 서비스를 배포하기 위해 "/opt/deploy.yml" 구성 파일을 준비합니다.
 - b) 웹 서비스를 제거하기 위해 "/opt/rollback.yml" 구성 파일을 준비합니다.
 - c) int-srv 디바이스에서 다음 형식의 명령어 수행 시 타겟 호스트에 웹 서비스 배포 또는 제거가 자동으로 수행되어야 합니다.
`ansible-playbook /opt/{파일명}.yml -e "target={호스트네임}"`

라. 침입 탐지 시스템

- 1) web01에서 Suricata를 사용하여 구성합니다.
- 2) web01의 interface를 통해 들어오는 비정상적인 트래픽을 감시하도록 설정합니다.
- 3) 비정상적인 트래픽이 접근하였을 때 “abnormal traffic access” 이 나타나도록 구성합니다.

마. 로그 서비스

- 1) web02에서 Rsyslog를 활용하여 구성합니다.
- 2) fw, mail 디바이스의 로그는 web02의 /var/log/{Device Name}/system.log에서 확인가능하여야 합니다.
- 3) web02의 경우 TCP 방식으로 1514번 포트를 이용하여 통신합니다.
- 4) fw, mail의 경우 TCP 방식, 514번 포트를 이용하여 통신합니다.
- 5) fw, mail 로그를 효율적으로 관리하기 위해 아래의 정보를 참조하여 설정합니다.
 - a) /etc/logrotate.d/srv에서 진행합니다.
 - b) 한 로그 파일의 용량을 100MB로 제한합니다.
 - c) 최대 3개의 로그 파일을 보관하며 그 이후부터는 오래된 순으로 삭제하도록 구성합니다.
 - d) 과거의 로그 파일은 .gz 형식으로 저장되어야 합니다.

바. NTP 서비스

- 1) chrony를 활용하여 구성합니다.
- 2) NTP 서버는 prx로 지정합니다.
- 3) 보안 강화를 위해 NTP서비스에 MD5 키 기반 인증을 구성합니다.
 - a) 키 번호는 9번을 사용하며 Password는 Skill39**를 사용합니다.

F. client.ext.worldskills.org

가. 일반 구성

- 1) 이 장치는 서비스 테스트 클라이언트로 동작합니다.
- 2) 웹 및 메일 서비스를 이용할 수 있도록 클라이언트 패키지를 설치합니다.

나. 서비스 클라이언트

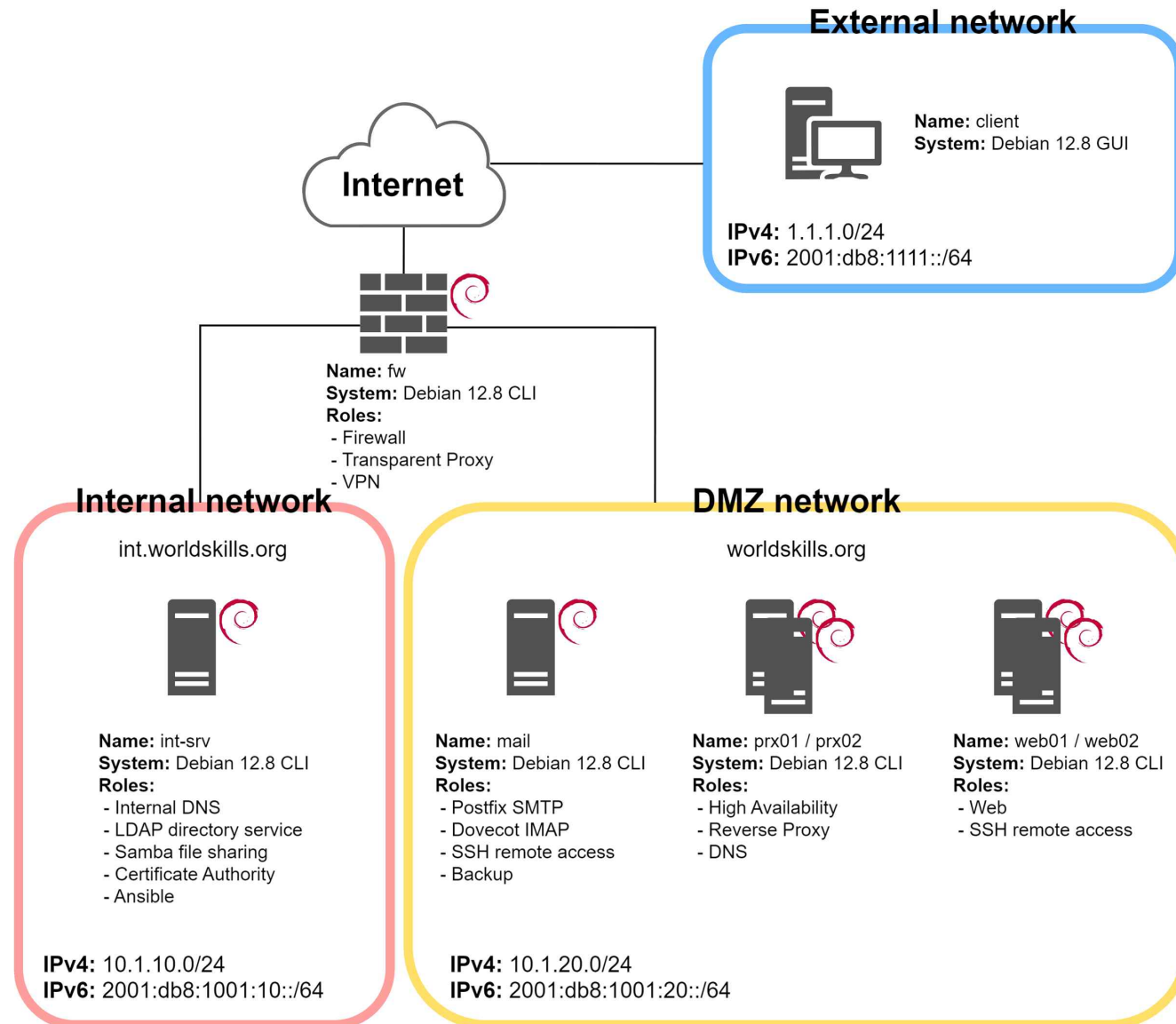
- 1) VPN 연결을 위한 NetworkManager 프로필을 추가합니다. VPN 연결 후 요구사항이 적절히 동작되는지 확인합니다.
- 2) 메일 클라이언트에 ws-user01 계정을 추가합니다.
- 3) 인증서 문제가 발생하지 않도록 루트 인증기관 인증서를 로컬 인증서 저장소 및 서드파티 인증서 저장소에 보관합니다.

다. NFS

- 1) /mnt/shares와 mail서버의 /root/shares 파일과 연결합니다.
- 2) 안전한 연결을 위해 Stunnel를 사용하여 구성합니다.
- 3) 서버와 클라이언트 간 NFS 통신은 SSL/TLS를 이용하여 Stunnel로 보호하도록 구성합니다.
- 4) Stunnel 포트의 경우, 65000번을 사용하여 서버와 통신할 수 있도록 구성합니다.

3. 부록

가. 네트워크 구성도



나. 시스템 구성표

Host	Perimeter	IPv4 Address	IPv6 Address	Roles
fw.worldskills.org	External	1.1.1.10/24	2001:db8:1111::10/64	Transparent proxy (squid), Firewall (nftables), VPN Server (WireGuard)
	Internal	10.1.10.1/24	2001:db8:1001:10::1/64	
	DMZ	10.1.20.1/24	2001:db8:1001:20::1/64	
	VPN	10.1.30.1/24	2001:db8:1001:30::1/64	
int-srv.int.worldskills.org	Internal	10.1.10.10/24	2001:db8:1001:10::10/64	DNS (BIND9), LDAP, File sharing (samba), Certificate Authority, Ansible
mail.worldskills.org	DMZ	10.1.20.10/24	2001:db8:1001:20::10/64	Mail (Postfix / Dovecot), Remote Access, Backup
prx.worldskills.org	DMZ	10.1.20.20/24	2001:db8:1001:20::20/64	Virtual IP, Reverse Proxy
prx01.worldskills.org	DMZ	10.1.20.21/24	2001:db8:1001:20::21/64	Reverse proxy, DNS (BIND9)
prx02.worldskills.org	DMZ	10.1.20.22/24	2001:db8:1001:20::22/64	Reverse proxy, DNS (BIND9)
web01.worldskills.org	DMZ	10.1.20.31/24	2001:db8:1001:20::31/64	Web, Remote Access
web02.worldskills.org	DMZ	10.1.20.32/24	2001:db8:1001:20::32/64	Web, Remote Access
client.ext.worldskills.org	External	1.1.1.20/24	2001:db8:1111::20/64	GUI environment, Client
	VPN	10.1.30.2/24	2001:db8:1001:30::2/64	