제 54회 전국기능경기대회 충남과제

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 직종명 | IT Network System | 과제명 | Linux Environment | 과제번호 | 제 1 과제 |
| 경기시간 | 4시간 | 비번호 |  | 심사위원  확인 | (인) |

# 과제 개요

당신은 항공권 티켓팅 서비스 제공 업체인 aflight의 네트워크 인프라 구축 담당자입니다. 인트라넷 상 사용자 계정 관리와 확장성, Single Sign On 기능을 활용하기 위한 Kerberos 기반의 솔루션을 적용하기로 했습니다. 자회사인 atrust와 트러스트를 통해 상호 간의 자원을 사용할 수 있고, 외근 직원을 위한 산업 표준 기반의 원격 접속 VPN을 구성합니다.

# 배포 자료(USB에 복사하여 배포)

### Debian Linux 9.8 DLBD 이미지

### Roundcube-1.3.8-complete.tar.gz

### Vmware Workstation 15 또는 상위 버전

# 주의 사항

### 암호를 필요로 하는 곳에 암호가 지정되지 않을 경우 “atc2019!”을 기본 값으로 사용합니다.

### 특별하게 지정되지 않은 옵션 또는 설정은 시스템이 추천하는 기본 값을 사용합니다.

### 정해진 USB장치 이외의 저장장치의 반입을 금지합니다.

### 휴대폰 등과 같은 스마트기기는 경기시작 전 심사위원(또는 관리 위원)에게 보관하도록 합니다.

### 채점 시 필요한 tcpdump 및 curl 패키지를 모든 리눅스 운영체제에 미리 설치합니다.

### GNOME이 설치된 호스트는 NetworkManager를 사용하도록 합니다.

# aflight.aero 과제 내용

## 운영체제 설치 및 네트워크 구성

#### 운영체제 설치

##### 부록의 운영체제 설치 항목을 참고하여 운영체제를 설치합니다.

##### 각 호스트의 IP주소 및 기타 환경을 설정합니다.

## af-1, af-2 작업 내용

#### DNS

##### aflight.aero에 대한 네임 서버를 구축합니다.

##### DHCP를 통해 할당 받은 주소를 동적으로 등록합니다.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 서버 | Name | Record | Value | Zone | Type |
| af-1, af-2 |  | SOA | af-1 | aflight.aero | Master  (af-2는 Slave) |
| af-1 | A | 10.47.0.1 |
| mail | A | 10.47.0.1 |
| af-2 | A | 10.47.0.2 |
| www | A | 10.47.145.1 |
| ldap | A | 10.47.145.1 |
| internal | A | 10.47.145.1 |
| ca | A | 10.47.145.1 |
|  | MX | mail |
| 전달자: 20.47.145.100 | | | atrust.com | forward |

#### Certification Authority (/etc/ssl/Aero-CA에 구성합니다.)

##### Atrust-CA의 하위 CA로 구성합니다.

##### CA 인증서의 Common name은 Aero-CA입니다.

##### 유효 기간은 5년입니다.

##### 인증서 해지 목록을 https://ca.aflight.aero/aero-ca.crl에 배포합니다.

##### 기관 정보 액세스(AIA) 중 CA Issuer는 https://ca.aflight.aero/aero-ca.crt에, OCSP는 https://ca.aflight.aero로 설정합니다.

##### af-1, af-2 간 CA가 설치된 디렉터리는 서로 동기화되어야 합니다.

#### MAIL (af-1에만 구성합니다.)

##### 메일 서비스를 위한 SMTPS와 IMAPS를 구성합니다.

##### 메일 서비스에 필요한 인증서는 Aero-CA에서 발급합니다.

##### LDAP 사용자 인증을 사용해야 합니다.

##### 보안상의 이유로 IMAP을 차단합니다.

#### WEB(Apache2)

##### internal.aflight.aero 웹 사이트는 office 호스트의 서브넷에서만 접근 가능합니다.

##### HTTPS를 지원하고, 인증서 오류가 표시되어서는 안 됩니다.

##### 웹 서비스에 필요한 인증서를 Aero-CA에서 발급하여 /etc/apache2/internal.crt로 저장합니다. SAN(internal.aflight.aero)이 포함되어 있어야 합니다.

##### /var/log/apache2/access.log에 접근 로그를 기록합니다.

##### 다음과 같은 웹 페이지를 표시합니다.

This is internal server.

##### www.aflight.aero 웹 사이트는 모든 네트워크에서 접근 가능합니다.

##### LDAP 인증에 의해 보호되어야 합니다.

##### HTTPS를 지원하고, 인증서 오류가 표시되어서는 안 됩니다.

##### 웹 서비스에 필요한 인증서를 Atrust-CA에서 발급합니다. SAN(www.aflight.aero)이 포함되어 있어야 합니다.

##### /var/log/apache2/access-www.log에 접근 로그를 기록합니다.

##### PHP를 이용해 다음과 같은 동적 웹 사이트를 표시합니다. [username]에는 인증한 LDAP 사용자가 표시되어야 합니다.

This is server www.aflight.aero. Welcome, [username]

#### LDAP

##### 도메인 내 사용자 계정을 저장하기 위한 디렉터리 서비스로 구성합니다. 사용자 추가는 아래 표를 참고합니다.

##### ou=aeros, dc=aflight, dc=aero

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| username | password | uid | gid | homedir | shell |
| aero01~99 | atc2019! | 1001~1099 | nogroup | /home/사용자 이름 | /bin/bash |

##### LDAP 서비스로 접근할 때는 GSSAPI를 통한 Kerberos 인증이 선행되어야 합니다.

##### admin@aflight.aero가 기존 cn=admin, dc=aflight, dc=aero을 대신합니다.

##### 두 서버 간 데이터베이스 내용은 서로 복제되어야 합니다.

#### Kerberos

##### LDAP, 웹 서비스, 로그인 인증을 위한 KDC 및 관리 서비스를 설치하고 구성합니다.

##### Kerberos 영역 데이터베이스로 LDAP을 사용합니다. 이에 필요한 Kerberos 컨테이너의 DN은 cn=krb5,dc=aflight,dc=aero입니다.

##### Kerberos를 통해 시스템 로그인이 가능해야 합니다.

##### Kerberos를 통해 PAM 인증 된 경우 GSSAPI를 통해 LDAP 서버에 접근하여 사용자 시스템 정보(homedir, uid, shell 등)를 불러와 사용자 로그인 시 적용되어야 합니다.

##### af-1과 af-2 모두 KDC로 구성합니다. 클라이언트에 af-1과 af-2 모두를 KDC로 설정 합니다.

##### 경기 중 Kerberos 티켓이 만료되지 않도록 적절한 설정(주기적인 갱신 등)을 합니다.

## af-srv 작업 내용

#### Reverse proxy

##### NGINX를 이용한 HTTP/HTTPS 리버스 프록시를 구성합니다.

##### af-1과 af-2에 Round-robin 되도록 합니다.

##### OCSP Stapling을 설정합니다. 올바른 OCSP 응답이 가능해야 합니다.

#### Load balancing

##### NGINX를 이용하여 LDAP을 위한 로드밸런싱을 구성합니다.

##### af-1과 af-2에 Round-robin 되도록 합니다.

#### DNS

##### 외부 응답 전용 DNS 서버를 구성합니다.

##### atrust.com 외부 레코드 응답도 가능하도록 전달자를 설정합니다.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 서버 | Name | Record | Value | Zone | Type |
| af-srv |  | SOA | ns | aflight.aero | Master |
| ns | A | 152.1.22.100 |
| www | A | 152.1.22.100 |
| ca | A | 152.1.22.100 |
| 전달자: 20.47.145.100 | | | atrust.com | forward |

## fw 작업 내용

#### DHCP

##### inside 인터페이스에서 DHCP 요청을 받습니다.

##### 할당할 IP 대역: 10.47.15.200~10.47.15.250/24

##### DNS: 10.47.0.1, 10.47.0.2

##### Default Gateway: 10.47.15.

##### af-1, 2의 DNS 서버에 할당된 IP 주소의 레코드를 동적으로 등록하도록 합니다.

#### Site-to-Site VPN

##### fw.aflight.aero – fw.atrust.com 간 StrongSWAN 패키지를 이용해서 IKEv2 VPN을 구성합니다.

#### NAT

##### 152.1.22.0/24가 출발지인 패킷 중 fw.aflight.aero 호스트의 HTTP, HTTPS, DNS로 향하는 패킷을 af-srv.aflight.aero으로 DNAT 합니다.

##### 내부 클라이언트의 네트워크에서 outside 인터페이스로 나가는 패킷은 인터페이스의 주소로SNAT 합니다.

# ATURST.COM 과제 내용

## 운영체제 설치 및 네트워크 구성

#### 운영체제 설치

* + - 부록의 운영체제 설치 항목을 참고하여 운영체제를 설치합니다.
    - 각 호스트의 IP주소 및 기타 환경을 설정합니다.

## at-1 작업 내용

#### Certification Authority (/etc/ssl/Atrust-CA에 구성합니다.)

##### 최상위 인증기관으로 구성합니다.

##### CA 인증서의 Common name은 Atrust-CA입니다.

##### 유효 기간은 5년입니다.

#### DNS

##### 과제에 필요한 레코드를 등록합니다.

##### 내부 View는 atrust.com, aflight.aero 내의 호스트만 쿼리 가능합니다.

##### 과제에 필요한 레코드는 다음 표를 참고합니다.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| View | Name | Record | Value | Zone | Type |
| 외부 View | ns | A | 152.1.22.200 | atrust.com | Master |
| ra | A | 152.1.22.200 |
| 내부 View | ns | A | 20.47.145.100 |
| at-1 | A | 20.47.145.100 |
| www | A | 20.47.145.100 |
| mail | A | 20.47.145.100 |
| webmail | A | 20.47.145.100 |
|  | MX | mail |
| 전달자: 10.47.0.1, 10.47.0.2 | | | aflight.aero | forward |

#### MAIL

##### 메일 서비스를 위한 SMTPS와 IMAPS를 구성합니다.

##### 메일 서비스에 필요한 인증서는 Atrust-CA에서 발급합니다.

##### 보안상의 이유로 IMAP을 차단합니다.

##### DataBase 사용자 인증을 사용해야 합니다.

##### At-1에서 “bigmail”이라는 커맨드를 입력하면 현재 메일박스에 있는 메일들을 검사하여 메일의 크기가 5MB 이상인 메일들을 ‘지운 메일함’으로 옮기고, 플래그를 추가하도록 구성합니다.

#### Webmail

##### AT-1에 배포자료를 이용해 roundcube를 설치하고 /var/www/roundcube에 구성하도록 합니다. 또한, 한국 사용자의 편의성을 위해 해당 페이지는 한글로 출력되게 구성하도록 합니다.

##### Roundcube 페이지는 https://webmail.atrust.com을 통해 접근이 가능해야하고, Atrust-CA에서 발급된 인증서를 사용해 암호화되어야합니다.

#### WEB(nginx)

##### http://www.atrust.com 웹 사이트 접속 시 Radius를 통해 사용자 인증이 가능해야 합니다.

##### PHP를 이용해 다음과 같은 동적 웹 사이트를 표시합니다. [hostname]에는 현재 응답한 서버의 호스트 이름이 표시되고, [username]에는 인증한 radius 사용자가 표시되어야 합니다.

##### At-1에는 apache2가 설치되어있으면 안됩니다.

This is server [hostname]. Welcome, [username]

#### Database(postgresql)

##### db 데이터 베이스를 생성합니다.

##### ‘admin’을 암호로 사용하는 admin 사용자를 추가하고, 모든 호스트가 SSL 연결을 사용하도록 구성합니다. SSL 연결에 필요한 인증서는 Atrust-CA에서 발급하도록 합니다.

##### 도메인 내 사용자를 위한 “passwd\_table” 테이블을 생성합니다. 사용자 추가는 아래 표를 참고하도록 합니다.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| username | password | uid | Gid | homedir | shell |
| trust01~09 | x | 1001~1009 | nogroup | /home/사용자 이름 | /bin/bash |

#### Database(Mariadb)

##### db 데이터 베이스를 생성합니다.

##### ‘admin’을 암호로 사용하는 admin 사용자를 추가하고, SSL 연결을 사용하도록 구성합니다. SSL 연결에 필요한 인증서는 Atrust-CA에서 발급하도록 합니다.

##### Radius 서비스를 위한 “radcheck” 테이블을 생성하고, Radius 서비스에서 사용할 유저를 추가하도록 합니다.

##### 쿼리에 대한 로그를 /var/log/mysql/query.log에 남기도록 합니다.

##### Af-srv를 슬레이브 서버로 구성하여 데이터를 백업하도록 합니다. 이를 위해 추가로 ssl 연결을 지원하고 ‘replica’를 암호로 사용하는 replica 사용자를 생성하여 Af-srv는 해당 유저를 통해 at-1과 암호화된 통신을 할 수 있도록 구성합니다.

##### SSL 구성 시, 암호화 알고리즘은 기본 값을 사용하여 구성합니다.

#### Radius

##### 공유 암호는 atc2019!를 사용합니다.

##### 유저 정보를 MariaDB를 통하여 받아와야합니다. 또한, MariaDB에 접근할 때에는 admin 유저를 사용하여 SSL 연결을 하도록 구성합니다.

##### 시스템 로그인 시 Radius를 이용해 PAM 인증을 하도록 구성합니다

##### SSL 암호화 구성 시, 암호화 알고리즘은 기본 값을 사용하여 구성합니다.

## fw 작업 내용

#### DHCP

##### inside 인터페이스에서 DHCP 요청을 받습니다.

##### 할당할 IP 대역: 20.47.145.200~20.47.145.230/24

##### DNS: 20.47.145.100

##### Default Gateway: 20.47.145.254

##### at-1의 DNS 서버에 할당된 주소 레코드를 등록하도록 합니다.

#### Site-to-Site VPN

##### fw.aflight.aero – fw.atrust.com 간 IKEv2 VPN을 구성합니다.

#### Remote Access VPN

##### 외부에서 내부 서비스 이용이 가능하도록 IKEv2 기반의 원격 접속 VPN을 구성합니다.

#### NAT

##### 152.1.22.0/24가 출발지인 패킷 중 fw.atrust.com 호스트의 DNS 서비스로 향하는 패킷을 at-1.atrust.com 호스트로 DNAT 합니다.

##### 클라이언트가 속한 네트워크에서 outside 인터페이스로 나가는 패킷은 SNAT 합니다.

# 클라이언트 설정

## office 작업 내용

#### Kerberos ticket을 이용해 Web 서비스에 싱글 사인 온이 가능해야 합니다.

#### Kerberos를 통해 bash쉘 및 GNOME 세션에 login이 가능해야 합니다.

#### curl을 설치합니다.

#### Openpgp를 통해 송수신하는 메일을 암호화합니다.

#### Icedove를 설치하고, aero01 유저를 추가합니다.

#### ldap-utils를 설치합니다.

## branch 작업 내용

#### Radius를 통해 bash쉘 및 GNOME 세션에 login이 가능해야 합니다.

#### Openpgp를 통해 송수신하는 메일을 암호화합니다.

#### Mariadb-client를 설치하고 구성합니다.

#### Postgresql-client를 설치하고 구성합니다.

#### Webmail을 통해 trust01 유저를 추가합니다.

#### curl을 설치합니다.

## remote 작업 내용

#### DNS: 152.1.22.100

#### curl을 설치합니다.

#### 사용자의 Bash 쉘에서 vpn up을 입력하면 IKEv2 VPN에 연결하고 20.0.0.0/24 대역의 주소를 할당 받아 내부 서비스를 이용할 수 있게 합니다.

#### 사용자의 Bash 쉘에서 vpn down을 입력하면 VPN 연결을 해제하도록 합니다.

# 호스트 설정 표

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Hostname | OS installation | Interface name | IP address | Domain |
| af-1 | Debian Linux 9.5 no GUI | 기본 값 | 10.47.0.1/24 | aflight.aero |
| af-2 | Debian Linux 9.5 no GUI | 기본 값 | 10.47.0.2/24 |
| af-srv | Debian Linux 9.5 no GUI | server | 10.47.0.254/24 |
| service | 10.47.145.1/24 |
| office | Debian Linux 9.5 with GNOME | 기본 값 | DHCP |
| fw | Debian Linux 9.5 no GUI | inside | 10.47.15.1/24 |
| dmz | 10.47.145.254/24 |
| outside | 152.1.22.100/24 |
| at-1 | Debian Linux 9.5 no GUI | 기본 값 | 20.47.145.100/24 | atrust.com |
| fw | Debian Linux 9.5 no GUI | inside | 20.47.145.254/24 |
| outside | 152.1.22.200/24 |
| branch | Debian Linux 9.5 with GNOME | 기본 값 | DHCP |
| remote | 기본 값 | 152.1.22.50/24 | 없음 |

# 네트워크 구성도

