기술보안운영 과제 - 보안솔루션 가상 인프라 환경 구축하기

가상 시나리오 배경

OOO 기업에서는 사내 보안 인프라를 구축하고 고객들을 위한 웹서비스를 운영할 방침이다. 운영을 위한 서버는 서비스를 기준으로 내부 직원 PC 관리를 위한 내부DMZ 망과 외부 고객을 위한 웹 서비스가 운영되는 웹 서버 또는 데이터베이스 등이 위치할 외부 DMZ 망을 별도로 구성한다.
직원들의 PC와 내부DMZ 망은 외부와의 통신을 단절하여 사전에 외부로 유출할 수 있는 가능성을 차단하고자 하였고, 직원들의 PC의 위협 탐지를 위해 HIDS를 에이전트 방식으로 설치하여 이상 여부를 확인하는 서버를 구축한 뒤 위협을 모니터링 하고자 한다.
ㅇㅇㅇ 기업은 외부의 웹사이트를 개방하여 고객들 일부를 위한 웹서비스를 제공하고 이 웹서비스는 개발자만 접근할 수 있도록 통제하여 개발자가 내부망에서만 접근 및 개발 수정을 할 수 있도록 지정하고 나머지의 접근은 차단하고자 한다.

보안 수준 강화를 위하여 보안 인프라 구축 시 필요하지 않은 연결에 대해서는 모두 사전 차단할 예정이고, 외부 DMZ 망 영역에 존재하는 서버들은 중앙에서 방화벽에 의한 개별적 통제를 받아 처리하며, 방화벽이 보안 인프라를 구성하는 가장 핵심적인 백본 통신망으로써 구성되어 적절한 관리 통제를 위한 핵심적 요소로 자리 매김해야 한다.

핵심이 되는 방화벽이 중요한 만큼 방화벽의 접근 통제는 오직 관리자에 의해서만 접근과 수정이 가능하며 그 어떠한 연결도 허용하지 않도록 보안을 철저히 한다.

기술보안운영 과제 - 보안솔루션 가상 인프라 환경 구축하기

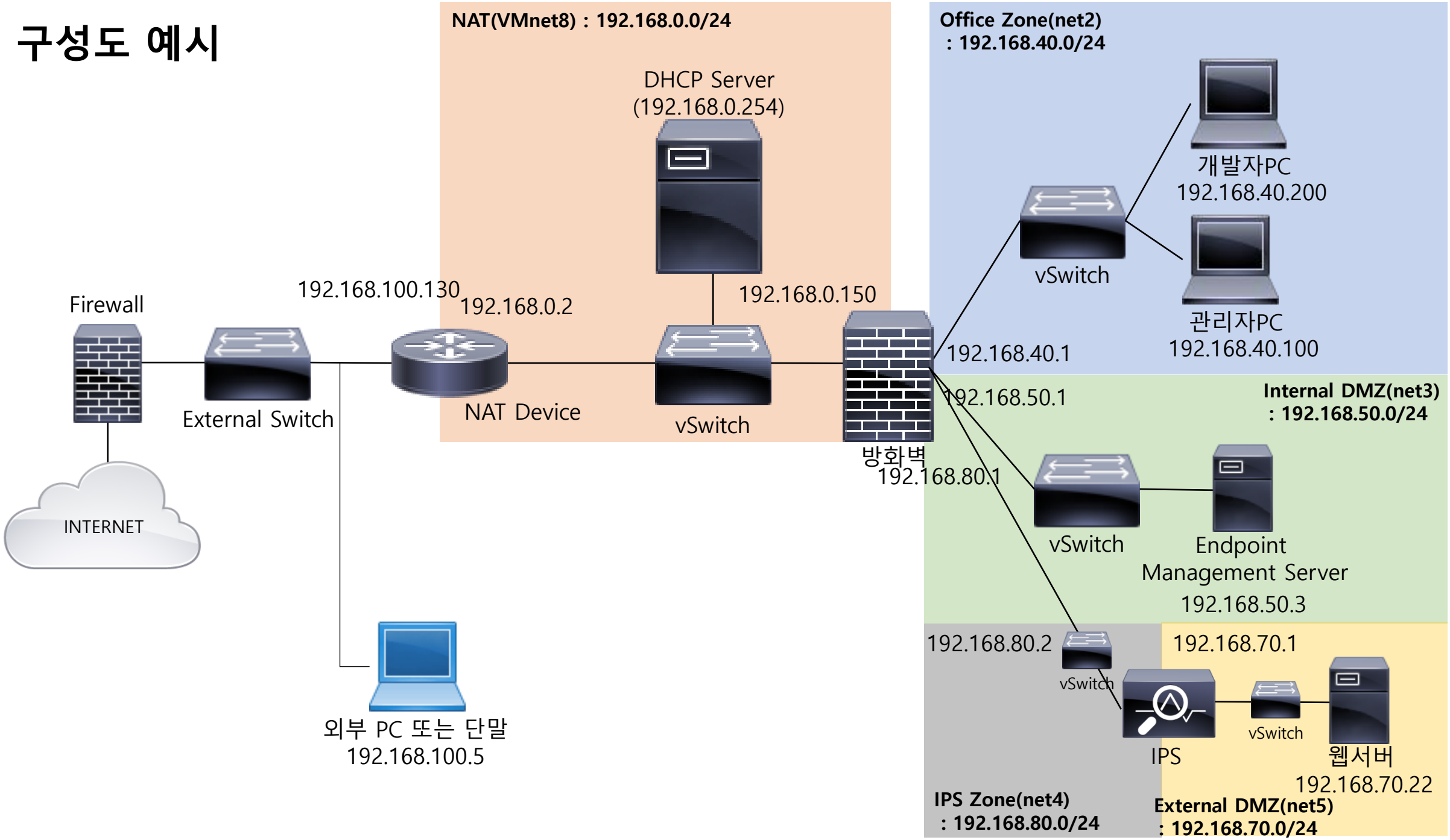
인프라 구성

① 네트워크 통신 장비(vSwitch 등)를 제외한 이미지 총 6개
(방화벽, IPS, 개발자PC, 관리자PC, 웹서버, 관리 서버(Endpoint Management Server))
② 통신망은 외부 인터넷, 외부(External) DMZ, 내부(Internal) DMZ, 오피스망(Office Zone)으로 구분
③ 각 통신은 최소한의 원칙에 따라 구성되어야 하며, 필요하지 않은 보안 정책은 제외하여 접근 통제를 수행
④ 관리 서버는 보안 솔루션인 OSSEC(HIDS 솔루션)의 서버로 활용하며, Agent는 개발자 또는 관리자 PC에서 설치
⑤ 웹 서버는 단일 기본페이지만 존재해도 가능(단 기본 페이지에 본인의 이름이 들어갈 것.)
⑥ 방화벽의 종류와 가상머신의 종류, OS 종류, GNS 활용 등의 제한 없음
(단 OSSEC은 리눅스 계열, 사용자 PC는 윈도우 계열로 고정)

접근 통제 규정 / 산출물(모든 산출물은 구성이 최종 완료된 후에 제출, 단계별 수행에 따른 제출이 아님)

① 방화벽의 모든 접근 통제는 화이트리스트 기반(All Deny) / **방화벽 정책 최종본 전체 적용 스크린샷 또는 룰**
② 웹 서버는 외부(구축되는 호스트PC의 외의 다른 장비(예: 휴대폰, 노트북 등))에서 HTTP 접속이 가능해야 함
/ 외부 PC에서 웹 브라우저를 통해 웹 페이지 **접속 사진(외부 휴대폰이나 다른 장비로 촬영)**
③ 웹 서버는 오피스망의 개발자PC만 HTTP 포트와 SSH 포트 접속이 가능해야 함 / **개발자PC에서 웹 서버 페이지 접속 스크린샷, SSH 터미널 접속 스크린샷 총 2개**
④ 관리 서버는 에이전트 정책 관리를 위해 오피스망 단말 전체를 대상으로 필요한 포트만 활성
/ **OSSEC Agent 정상 작동 여부 확인 스크린샷**
⑤ 관리 서버의 수정과 서비스 관리를 위하여 관리자PC에서만 SSH 접속 가능하도록 설정
/ **관리자PC에서 SSH 접속 화면 스크린샷, 사용자PC에서 SSH 접속 불가능 증적 화면 스크린샷**
⑥ 방화벽 접근은 오직 관리자 PC에서만 접근 가능하며, 관련 설정은 초기 설정 외에 모두 관리자 PC에서만 수행
/ **관리자PC에서 방화벽 관리 페이지 접속 화면과 개발자PC에서 방화벽 관리 페이지 접속 불가능 화면 스크린샷** 총 2개
⑦ 내부의 있는 모든 망은 외부와의 인터넷이 불가능 / **포탈(google, naver) 등 페이지 접속 불가능 화면 스크린샷**

구성도 예시


NAT(VMnet8) : 192.168.0.0/24
DHCP Server
(192.168.0.254)
Office Zone(net2)
: 192.168.40.0/24
개발자PC
192.168.40.200
vSwitch
관리자PC
192.168.40.100
192.168.100.130
192.168.0.2
192.168.0.150
Firewall
192.168.40.1
External Switch
NAT Device
vSwitch
192.168.50.1
Internal DMZ(net3)
: 192.168.50.0/24
방화벽
192.168.80.1
vSwitch
Endpoint
Management Server
192.168.50.3
INTERNET
192.168.80.2
192.168.70.1
vSwitch
vSwitch
IPS
웹서버
192.168.70.22
외부 PC 또는 단말
192.168.100.5
IPS Zone(net4)
: 192.168.80.0/24
External DMZ(net5)
: 192.168.70.0/24