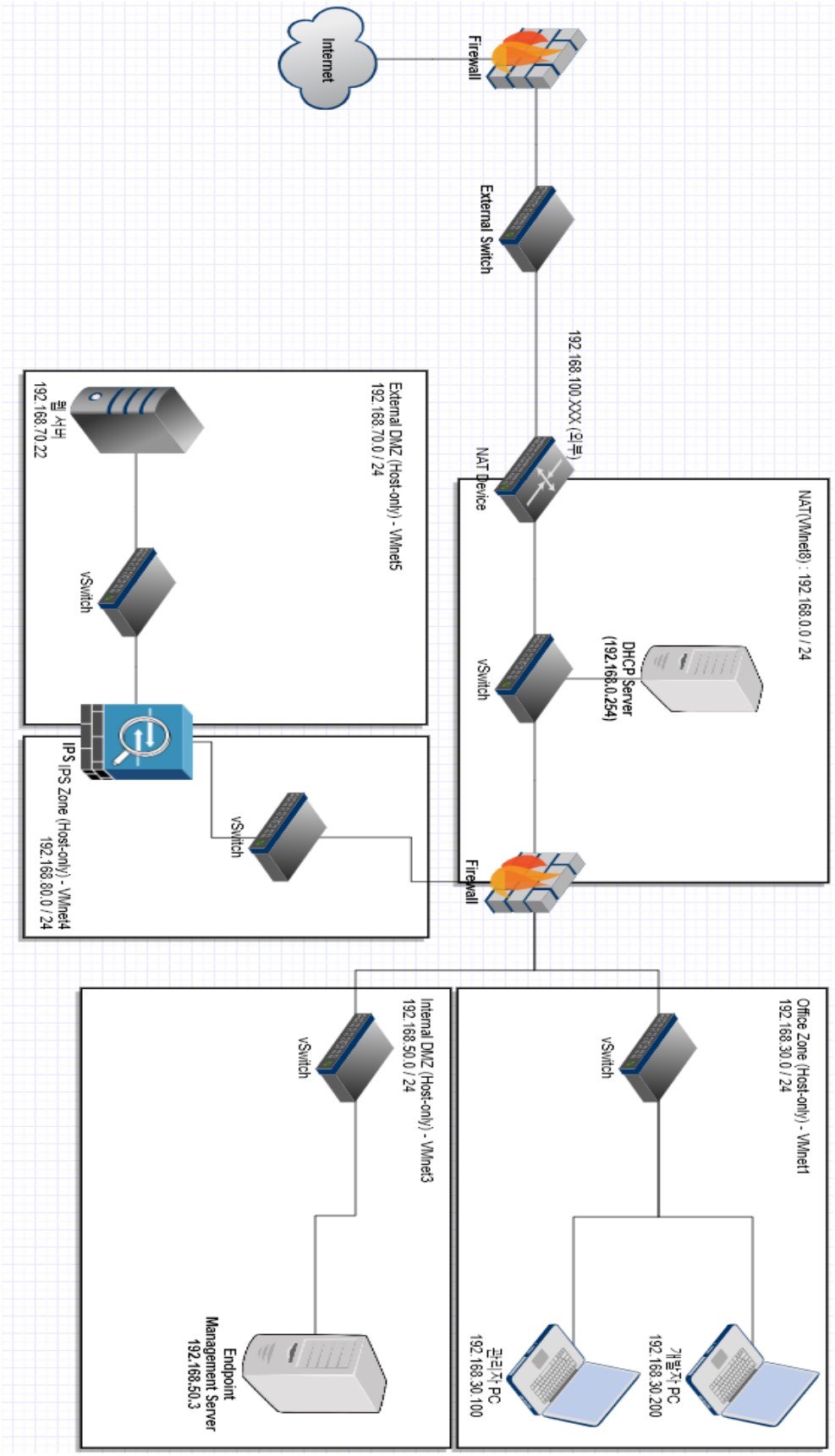
보안 솔루션 가상 인프라 환경 구축하기

이도원

[목차]

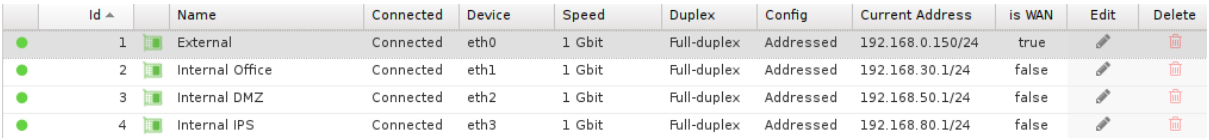
[인프라 구성도]


Internet
Firewall
External Switch
192.168.100.XXX (외부)
NAT Device
NAT(VMnet8) : 192.168.0.0 / 24
vSwitch
DHCP Server
(192.168.0.254)
Firewall
External DMZ (Host-only) - VMnet5
192.168.70.0 / 24
웹 서버
192.168.70.22
vSwitch
IPS
IPS Zone (Host-only) - VMnet4
192.168.80.0 / 24
vSwitch
Office Zone (Host-only) - VMnet1
192.168.30.0 / 24
vSwitch
개발자 PC
192.168.30.200
관리자 PC
192.168.30.100
Internal DMZ (Host-only) - VMnet3
192.168.50.0 / 24
vSwitch
Endpoint
Management Server
192.168.50.3

[인프라 구성 명세]

Firewall

영역	구분자	IP	OS	NIC
	External	192.168.0.150	Untangle	NAT
	Internal Office	192.168.30.1		VMnet 1
	Internal DMZ	192.168.50.1		VMnet 3
	Internal IPS	192.168.80.1		VMnet 4



Id	Name	Connected	Device	Speed	Duplex	Config	Current Address	is WAN	Edit	Delete
1	External	Connected	eth0	1 Gbit	Full-duplex	Addressed	192.168.0.150/24	true		
2	Internal Office	Connected	eth1	1 Gbit	Full-duplex	Addressed	192.168.30.1/24	false		
3	Internal DMZ	Connected	eth2	1 Gbit	Full-duplex	Addressed	192.168.50.1/24	false		
4	Internal IPS	Connected	eth3	1 Gbit	Full-duplex	Addressed	192.168.80.1/24	false		

NAT(VMnet 8) : 192.168.0 0 / 24

영역	구분자	IP	OS	NIC
NAT	DHCP Server	192.168.0.254		VMnet 8
	NAT Device	192.168.0.2		

Office Zone (VMnet 1_Host-only) : 192.168.30.0 / 24

영역	구분자	IP	OS	NIC
Office Zone	개발자 PC	192.168.30.200	Windows 7	VMnet 1
	관리자 PC	192.168.30.100	Windows 7	

Internal DMZ (VMnet 3_Host-only) : 192.168.50.0 / 24

영역	구분자	IP	OS	NIC
Internal DMZ	Endpoint Management Server	192.168.50.3	Ubuntu 14.04	VMnet 3

IPS Zone (VMnet 4_Host-only) : 192.168.80.0 / 24

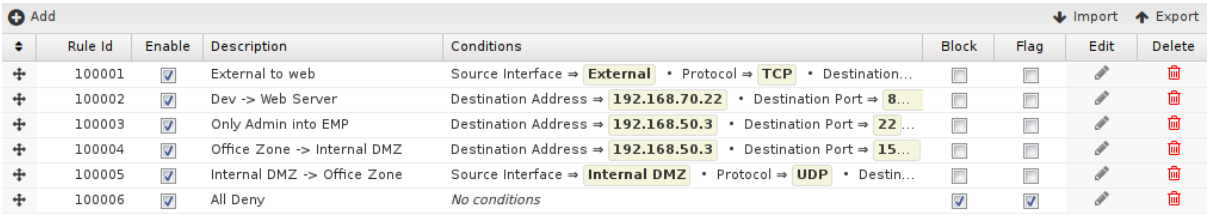
영역	구분자	IP	OS	NIC
IPS Zone	External (IPS)	192.168.80.2	Suricata	VMnet 4

External DMZ (VMnet 5_Host-only) : 192.168.70.22 / 24

영역	구분자	IP	OS	NIC
External DMZ	Web Server	192.168.70.22	Ubuntu 16.04	VMnet 5
	Internal (IPS)	192.168.70.1		

[접근 통제 구성 / 산출물]

1] 방화벽의 모든 접근 통제는 화이트 리스트 기반 (All Deny)



100001) External to web

- 외부에서 Web Server로 접속하는 것에 대한 허용 정책

- Source Interface : External / Protocol : TCP / Destination Address : 192.168.70.22 / Destination Port : 80

100002) Dev -> Web Server

- 개발자 PC에서 Web Server로 HTTP 포트, SSH 포트 접속 허용 정책

- Destination Address : 192.168.70.22 / Destination Port : 80, 22 / Protocol : TCP / Source Address : 192.168.30.200

100003) Only Admin into EMP(Endpoint Management Server)

- 관리자 PC에서 관리 서버로 SSH 접속 허용 정책

- Destination Address : 192.168.50.3 / Destination Port : 22 / Source Address : 192.168.30.100

100004) Office Zone -> Internal DMZ

100005) Internal DMZ -> Office Zone

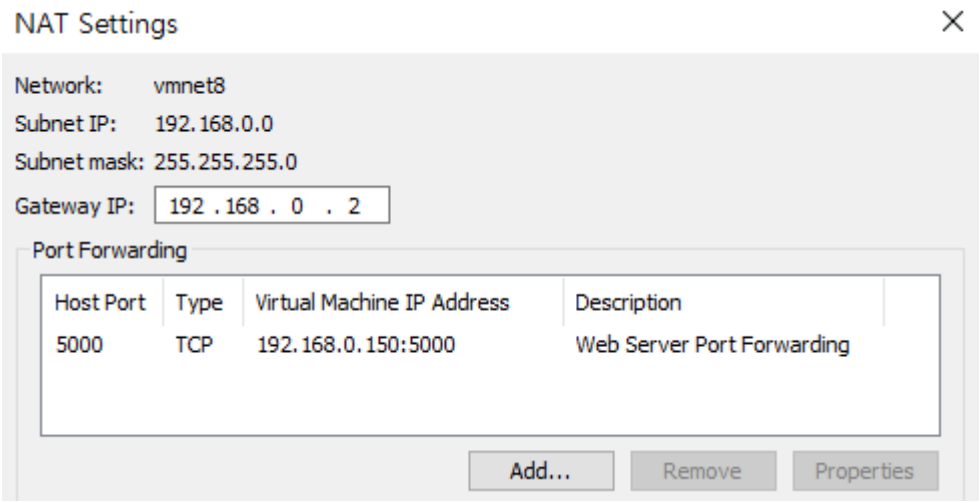
- 관리 서버는 에이전트 정책 관리를 위해 오피스망 단말 전체를 대상으로 필요한 포트 (1514/UDP)만 활성화

- Destination Address : 192.168.50.3 / Destination Port : 1514 / Protocol : UDP / Source Interface : Internal Office

- Source Interfaces : Internal DMZ / Protocol : UDP / Destination Port : 1514 / Destination Interface : Internal Office

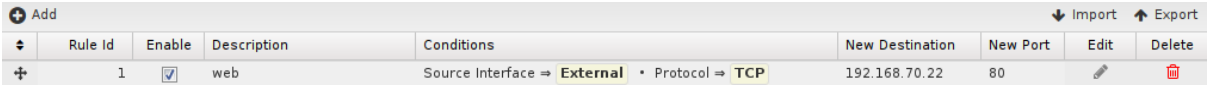
100006) All Deny

2] 웹 서버는 외부 (구축되는 호스트 PC의 외의 다른 장비 (예: 휴대폰, 노트북 등))에서 HTTP 접속이 가능해야한다.



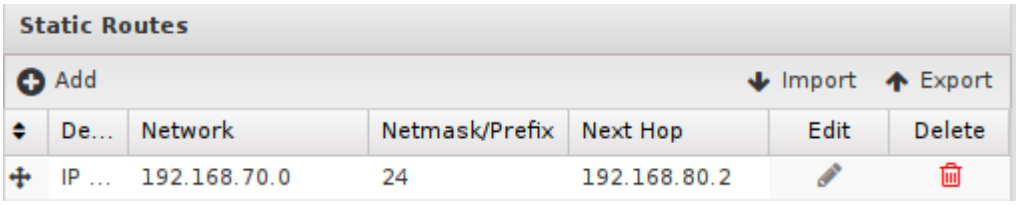
1) NAT Device Port Forwarding

- 외부 IP port : 5000으로 접속 시, Untangle(192.168.0.150)의 5000번포트로 포트포워딩 한다.



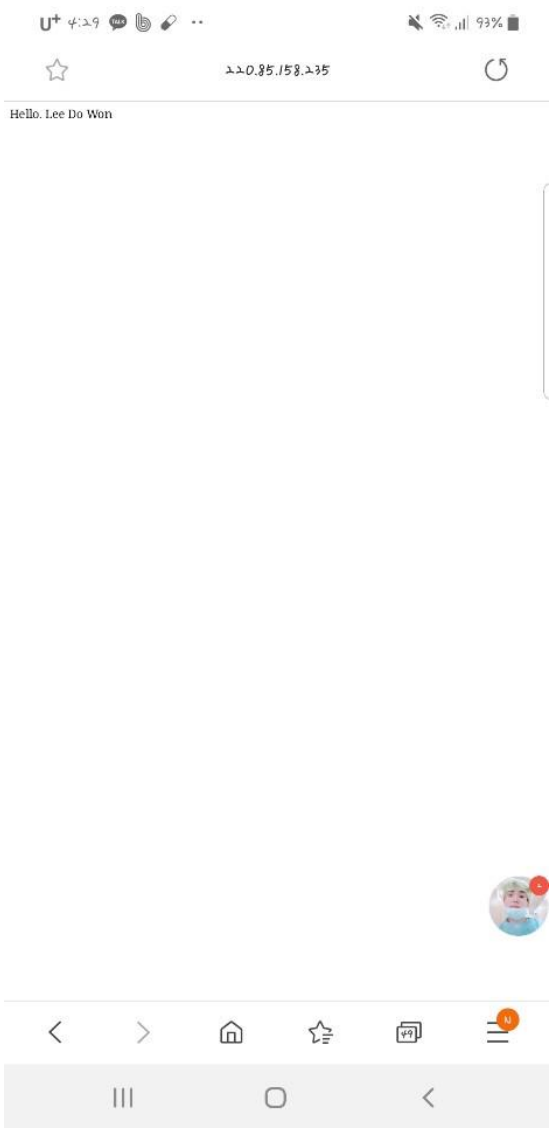
2) Untangle Port Forwarding

- 외부에서 –> 방화벽으로 포워딩 된 것들을 다시 192.168.70.22:80으로 포트포워딩 할 수 있게 규칙을 생성한다.



3) IP Forwarding

- External DMZ 구역과 IPS Zone을 라우팅 해준다.

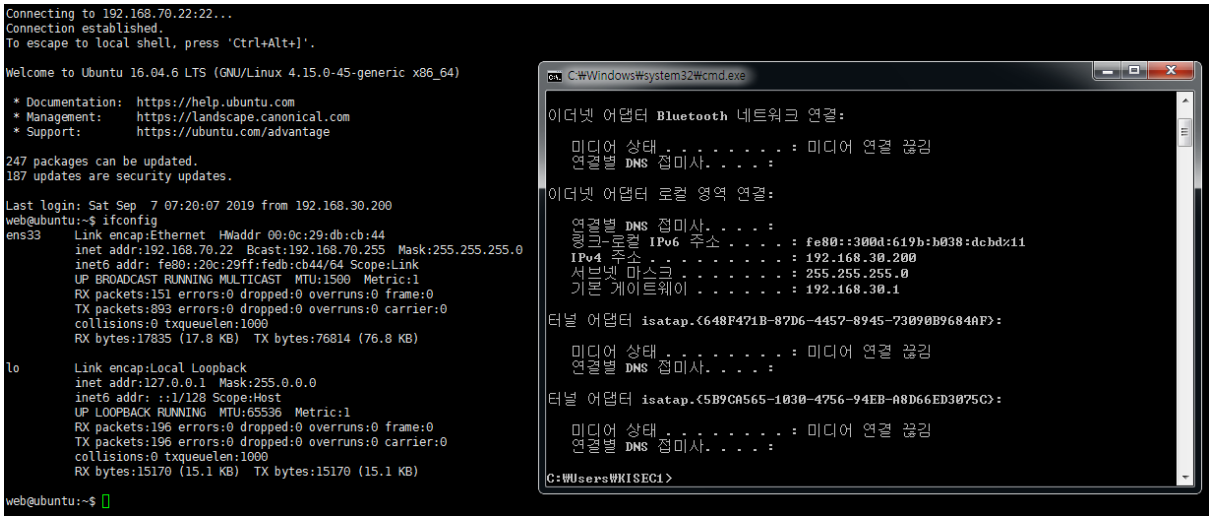


o

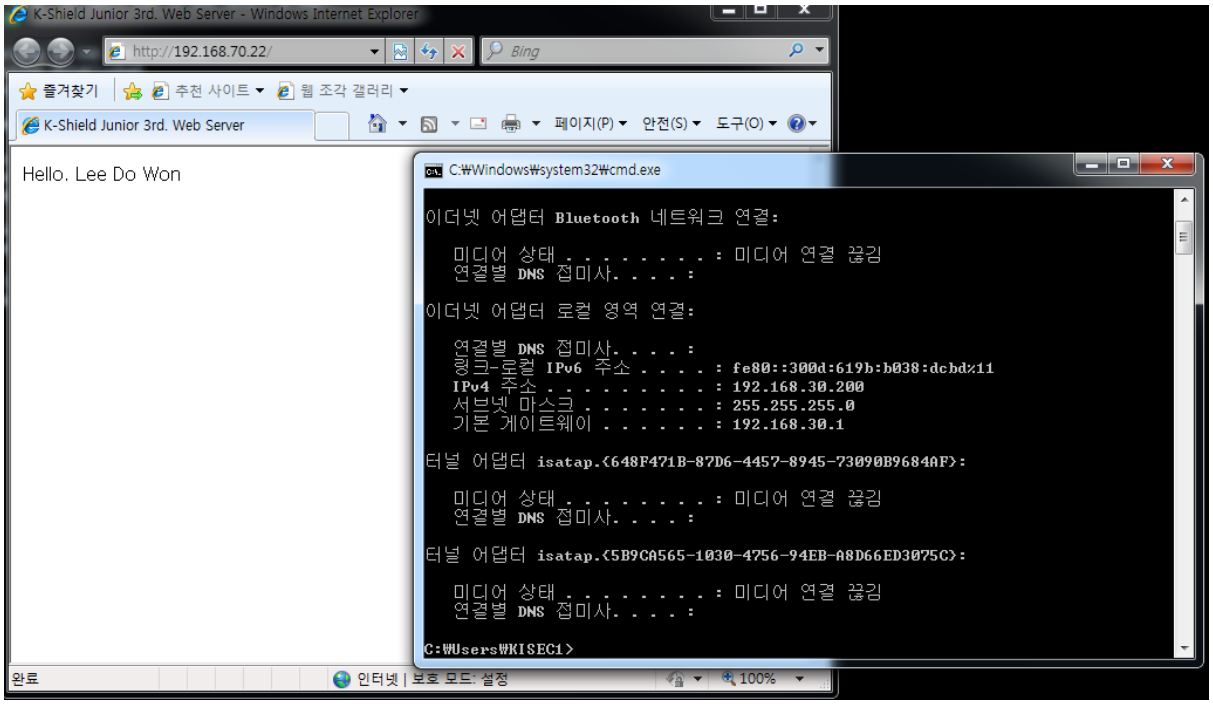
- 휴대폰에서 220.85.158.235:5000로 Web Server 접속 완료

3] 웹 서버는 오피스망의 개발자 PC만 HTTP 포트와 SSH 포트 접속이 가능해야 한다.

- 방화벽 접근 통제 규정은 1] 번의 Rule id : 100002를 참조 한다.



1) 개발자 PC(192.168.30.200) -> Web Server (192.168.70.22) SSH 접속 완료.



2) 개발자 PC(192.168.30.200) -> Web Server (192.168.70.22) 웹 서버 페이지 접속 완료.

4] 관리 서버는 에이전트 정책 관리를 위해 오피스망 단말 전체를 대상으로 필요한 포트만 활성화 한다.

- 방화벽 접근 통제 규정은 1] 번의 Rule id 100004, 100005를 참조한다.

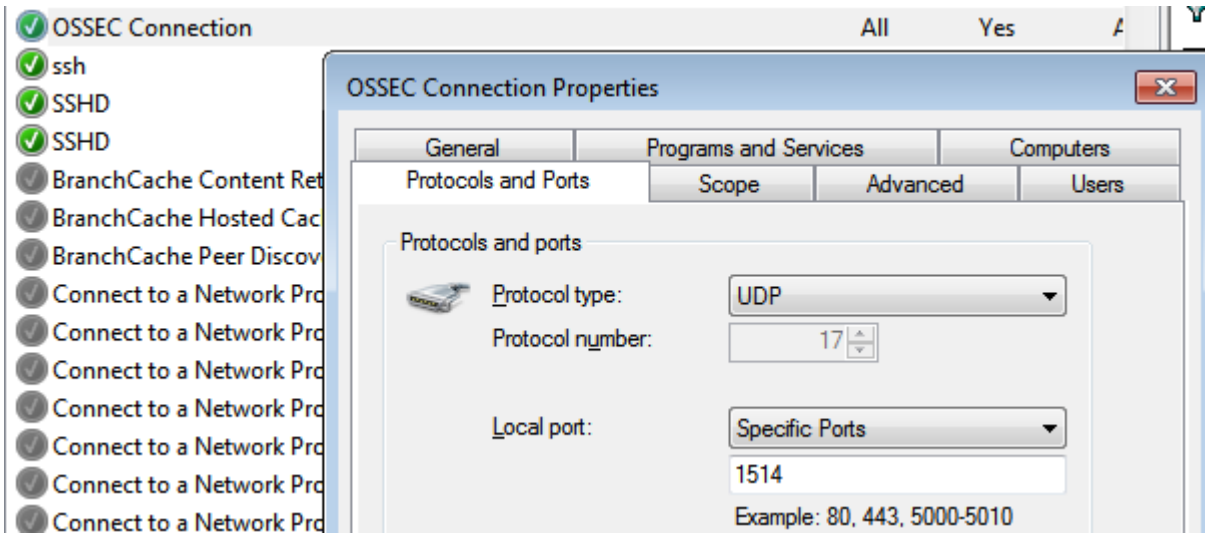
```
root@ubuntu:/var/ossec/bin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  192.168.30.200       anywhere             udp dpt:1514
ACCEPT     udp  --  192.168.30.100       anywhere             udp dpt:1514

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
```

- OSSEC 서버에서 OSSEC Agent (Office 망 단말 전체를 대상) UDP 1514 포트 허용 (인바운드)

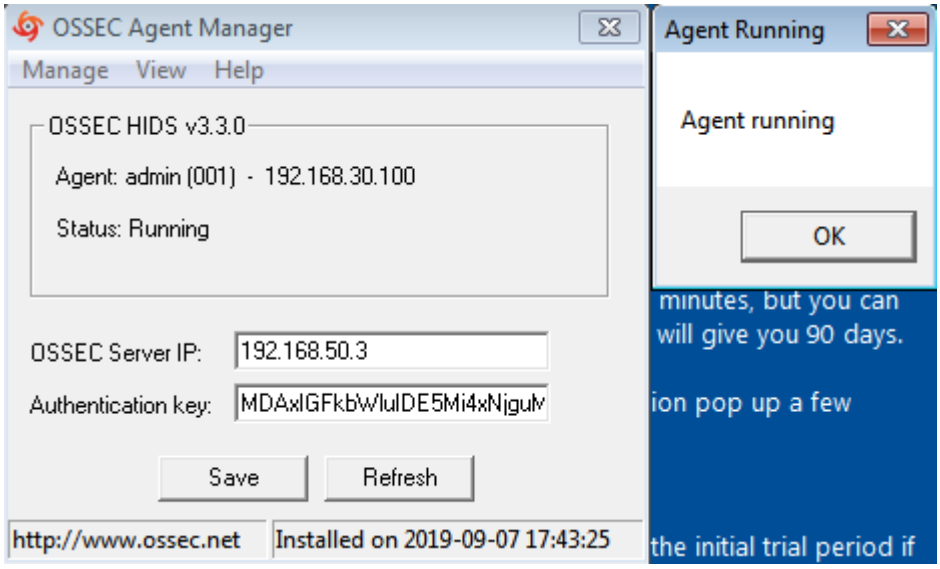
- 모든 아웃바운드 트래픽은 허용

- 개발자 PC와 관리자 PC로부터 UDP 1514 포트로의 접근을 허용

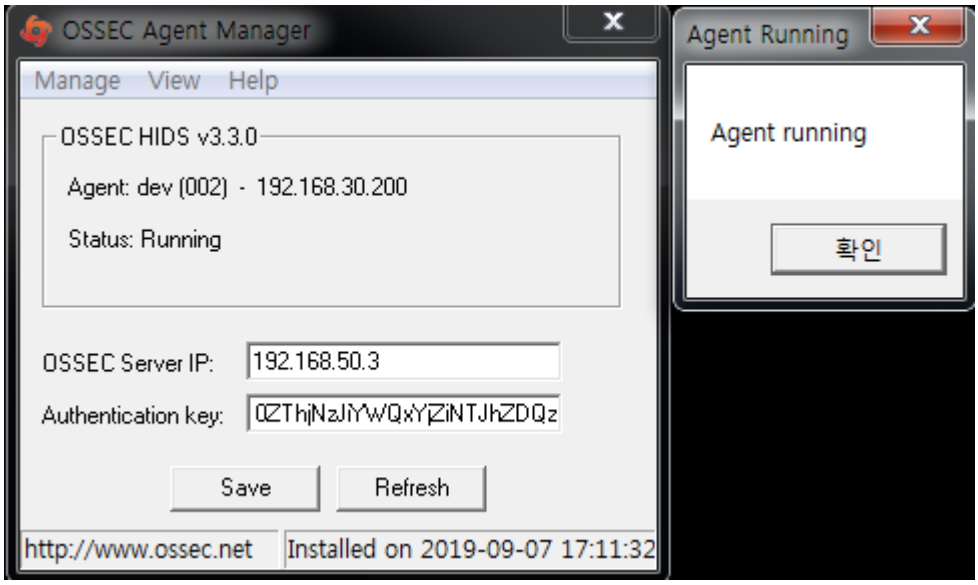
- 개발자 PC(Agent)에서의 UDP 1514 인바운드 규칙 생성



- 관리자 PC(Agent)에서의 UDP 1514 인바운드 규칙 생성



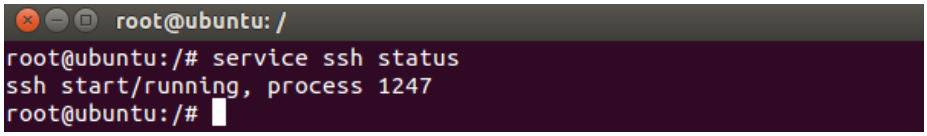
- 관리자 PC에서 OSSEC Agent 정상 작동 확인



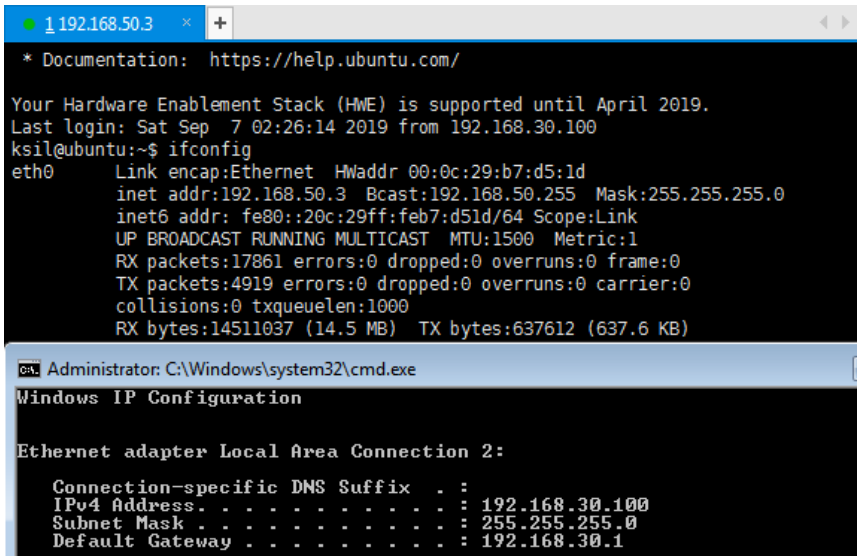
- 개발자 PC에서 OSSEC Agent 정상 작동 확인

5] 관리 서버의 수정과 서비스 관리를 위하여 관리자 PC에서만 SSH 접속 가능하도록 설정 한다.

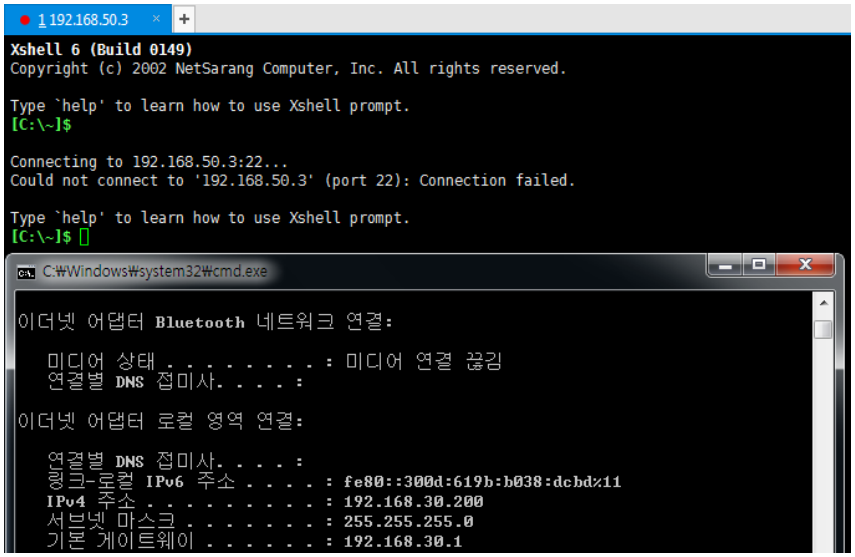
- 방화벽 접근 통제 규정 1] 번의 Rule id : 100003을 참조한다.



- 관리 서버에서 ssh 패키지 설치 후 가동 / 상태 확인

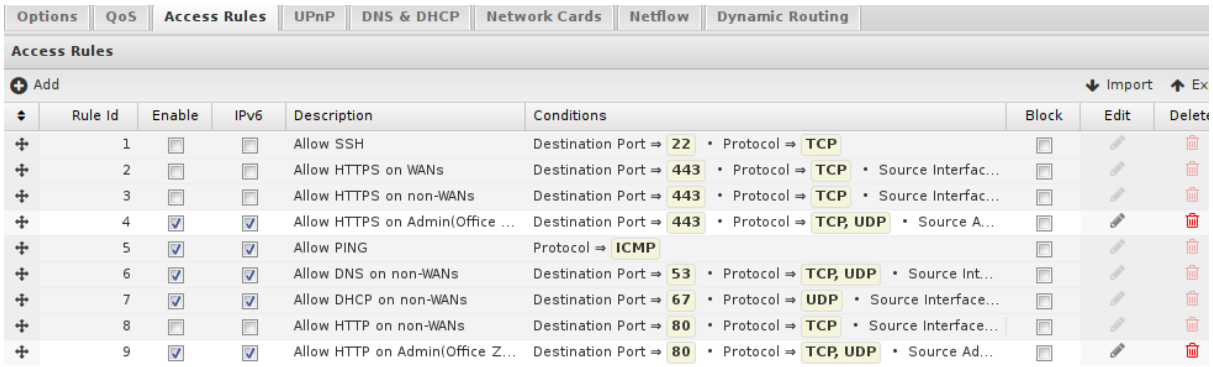


- 관리자 PC에서 SSH 접속 화면



- 개발자 PC에서 SSH 접속 불가능 화면

6] 방화벽 접근은 오직 관리자 PC에서만 접근 가능하며, 관련 설정은 초기 설정 외에 모두 관리자 PC에서만 수행 한다.



Untangle – Config – Network – Advanced – Access Rules에서

관리자 PC에서만 접근 가능하게 하기 위해 Allow HTTPS on non-WANs (Rule id : 3), Allow HTTP on non-WANs (Ruld id : 8)을 비활성화하고, 새로운 정책을 2개 추가한다.

4) Allow HTTPS on Admin(Office Zone)

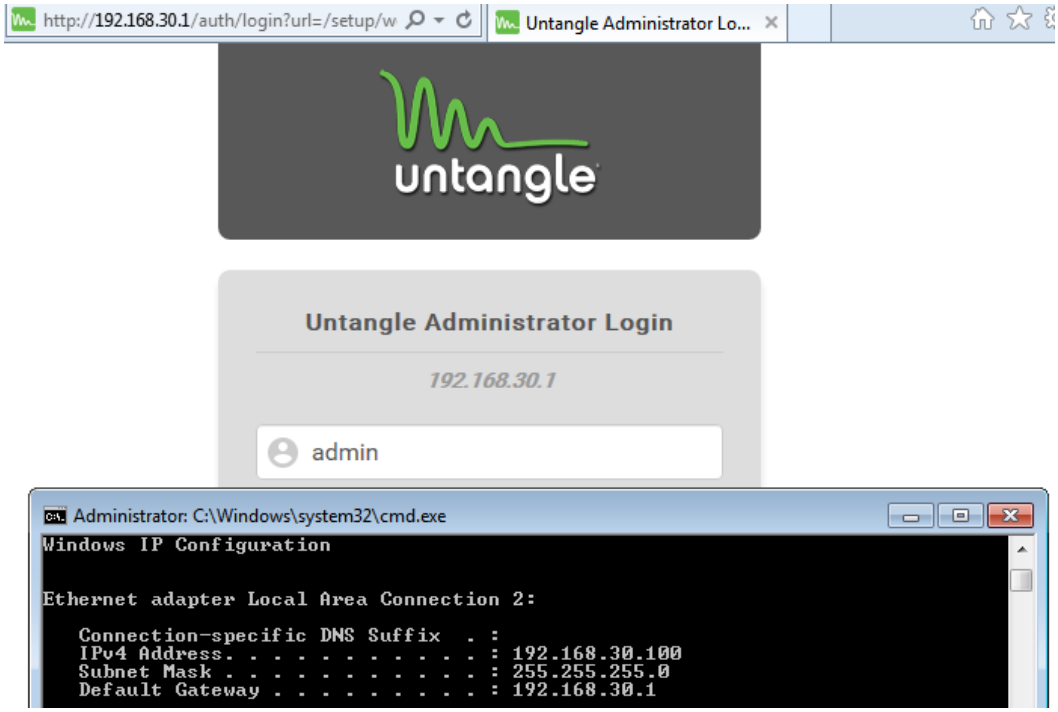
- 관리자에서의 HTTPS 접근을 허용하기 위해 정책을 설정

- Destination Port : 443 / Protocol : TCP, UDP / Source Address : 192.168.30.100

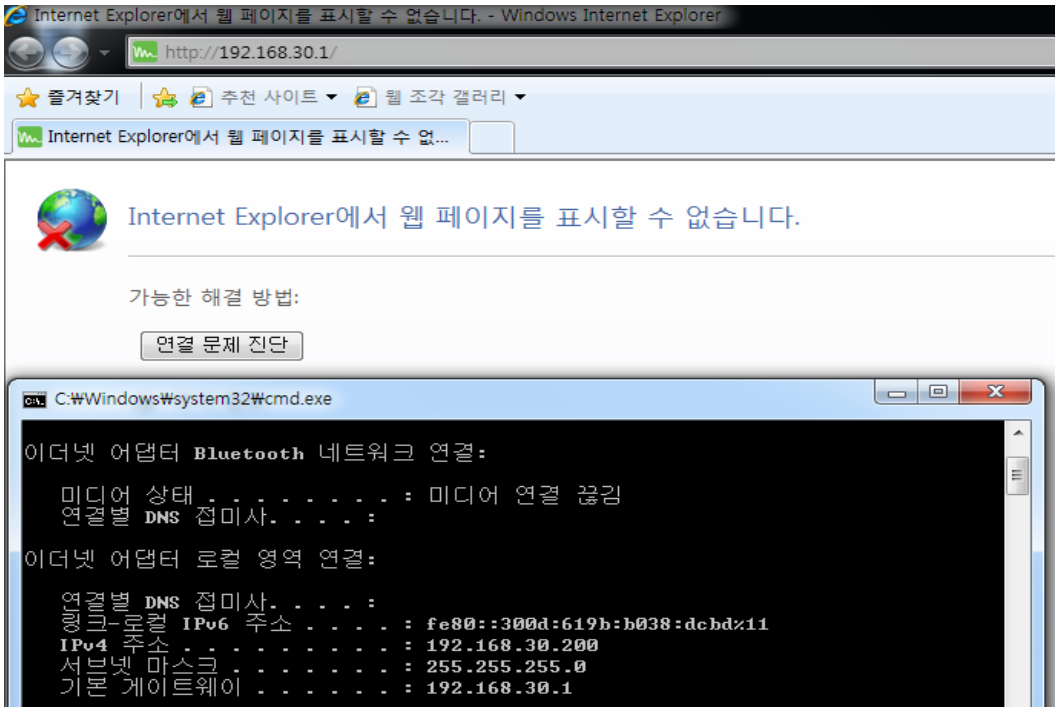
9) Allow HTTP on Admin(Office Zone)

- 관리자에서의 HTTP 접근을 허용하기 위해 정책을 설정

- Destination Port : 80 / Protocol : TCP, UDP / Source Address : 192.168.30.100

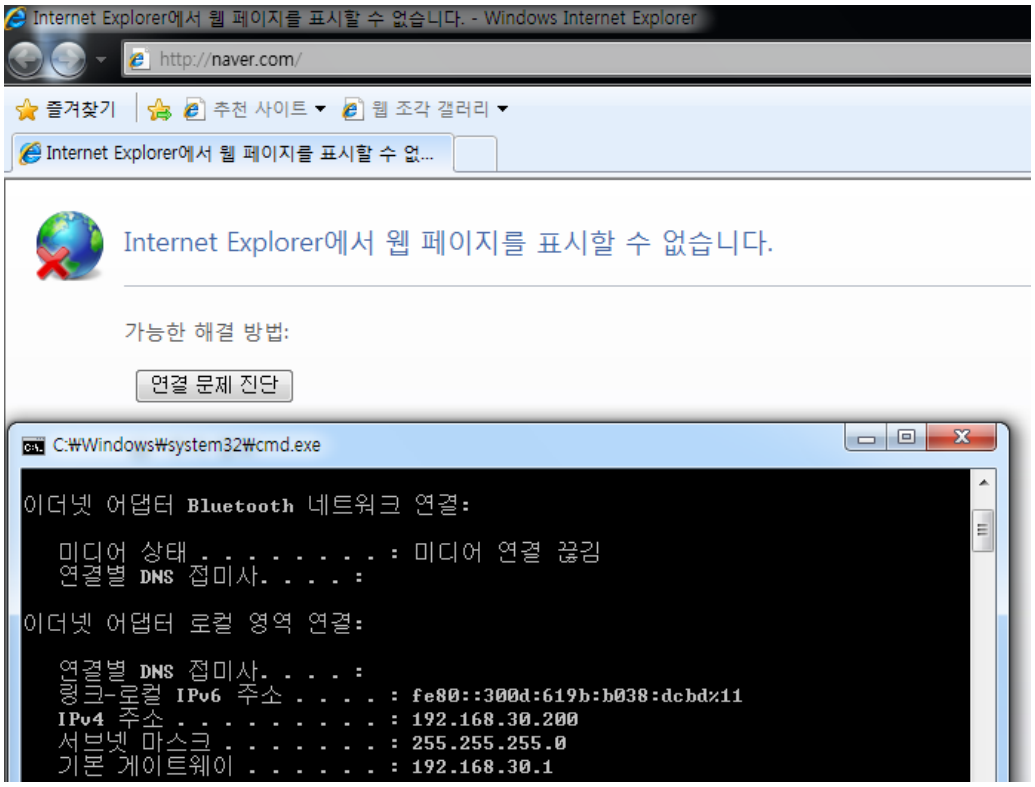


- 관리자 PC에서 방화벽 관리 페이지 HTTP 접속 완료

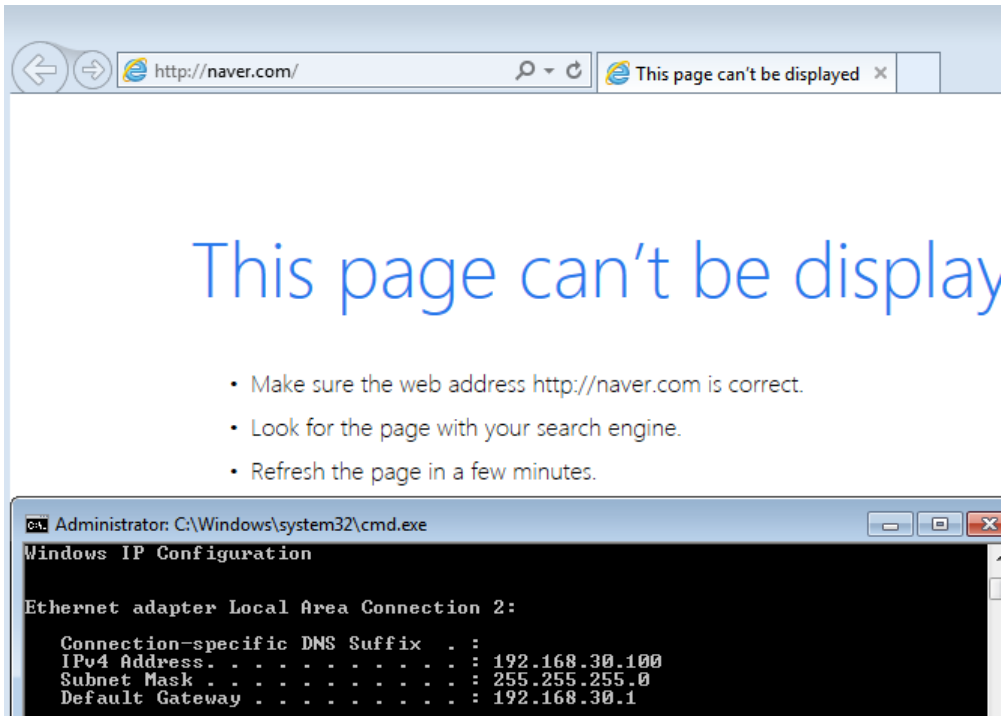


- 개발자 PC에서 방화벽 관리 페이지 접속 불가능

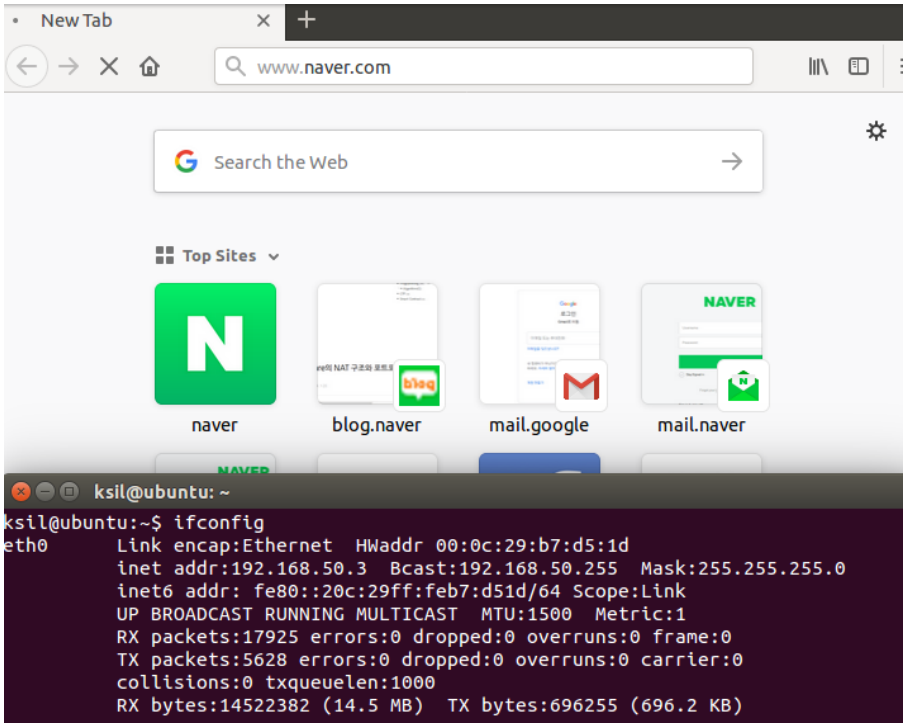
7] 내부의 있는 모든 망은 외부와의 인터넷이 불가능하다.



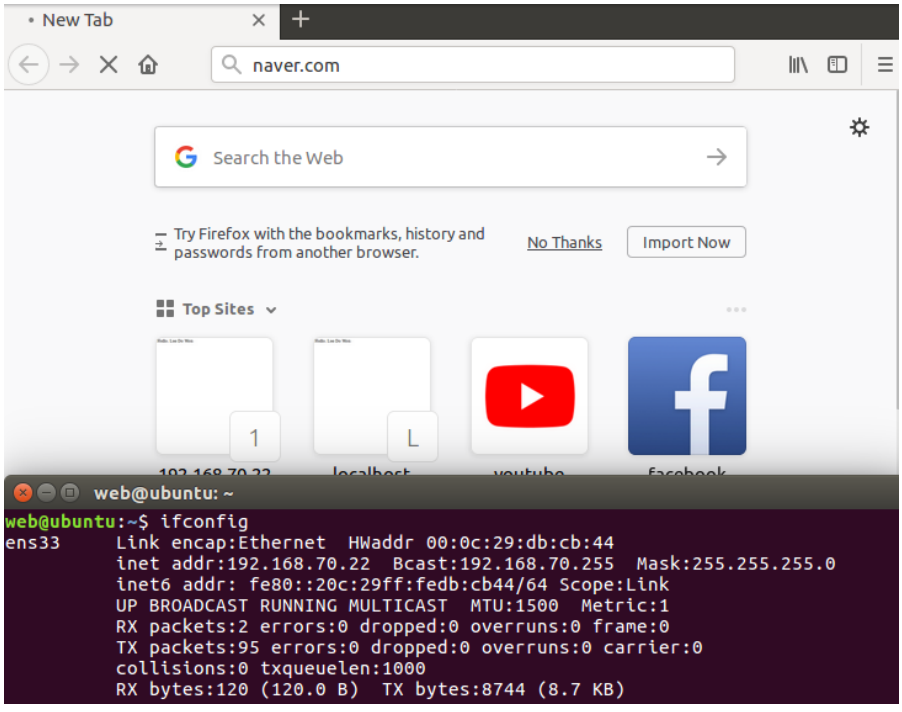
- Office Zone) 개발자 PC(192.168.30.200) 외부와의 인터넷 불가능



- Office Zone) 관리자 PC(192.168.30.100) 외부와의 인터넷 불가능



- Internal DMZ) Endpoint Management Server(192.168.50.3) 외부와의 인터넷 불가능



- External DMZ) Web Server(192.168.70.22) 외부와의 인터넷 불가능