

보안 솔루션 가상 인프라 환경 구축하기

이도원

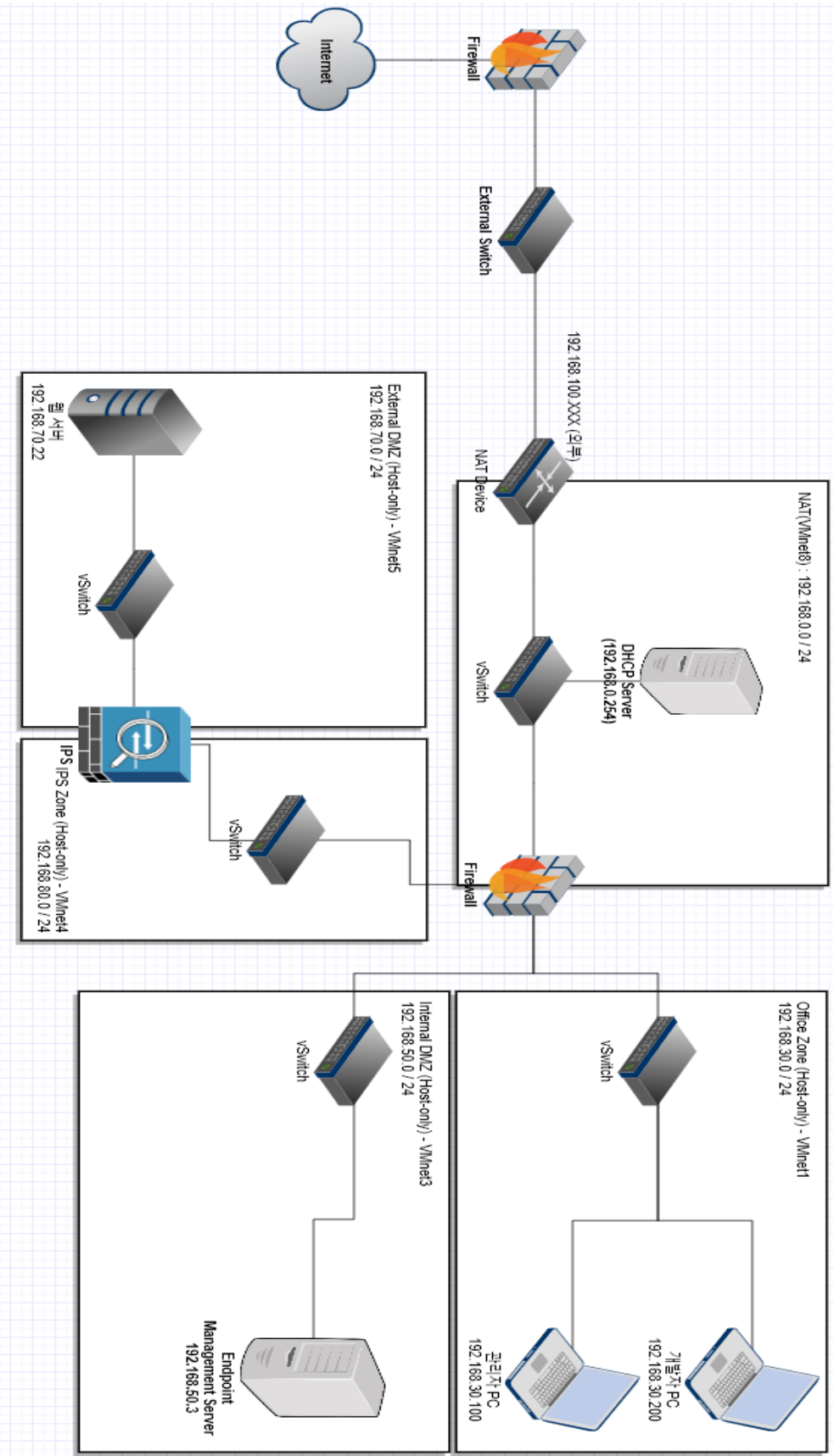
[목차]

1) 인프라 구성도

2) 인프라 구성 명세

3) 접근통제 구성 / 산출물

[인프라 구성도]



[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)

Add				Import Export					
	Rule Id	Enable	Description	Conditions	Block	Flag	Edit	Delete	
+	100001	<input checked="" type="checkbox"/>	External to web	Source Interface ⇒ External • Protocol ⇒ TCP • Destination...	<input type="checkbox"/>	<input type="checkbox"/>			
+	100002	<input checked="" type="checkbox"/>	Dev -> Web Server	Destination Address ⇒ 192.168.70.22 • Destination Port ⇒ 8...	<input type="checkbox"/>	<input type="checkbox"/>			
+	100003	<input checked="" type="checkbox"/>	Only Admin into EMP	Destination Address ⇒ 192.168.50.3 • Destination Port ⇒ 22...	<input type="checkbox"/>	<input type="checkbox"/>			
+	100004	<input checked="" type="checkbox"/>	Office Zone -> Internal DMZ	Destination Address ⇒ 192.168.50.3 • Destination Port ⇒ 15...	<input type="checkbox"/>	<input type="checkbox"/>			
+	100005	<input checked="" type="checkbox"/>	Internal DMZ -> Office Zone	Source Interface ⇒ Internal DMZ • Protocol ⇒ UDP • Destin...	<input type="checkbox"/>	<input type="checkbox"/>			
+	100006	<input checked="" type="checkbox"/>	All Deny	No conditions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			

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.

NAT Settings X

Network: vmnet8
 Subnet IP: 192.168.0.0
 Subnet mask: 255.255.255.0
 Gateway IP:

Port Forwarding

Host Port	Type	Virtual Machine IP Address	Description
5000	TCP	192.168.0.150:5000	Web Server Port Forwarding

1) NAT Device Port Forwarding

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

Add Import Export						
	Rule Id	Enable	Description	Conditions	New Destination	New Port
+	1	<input checked="" type="checkbox"/>	web	Source Interface ⇒ External • Protocol ⇒ TCP	192.168.70.22	80
					<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

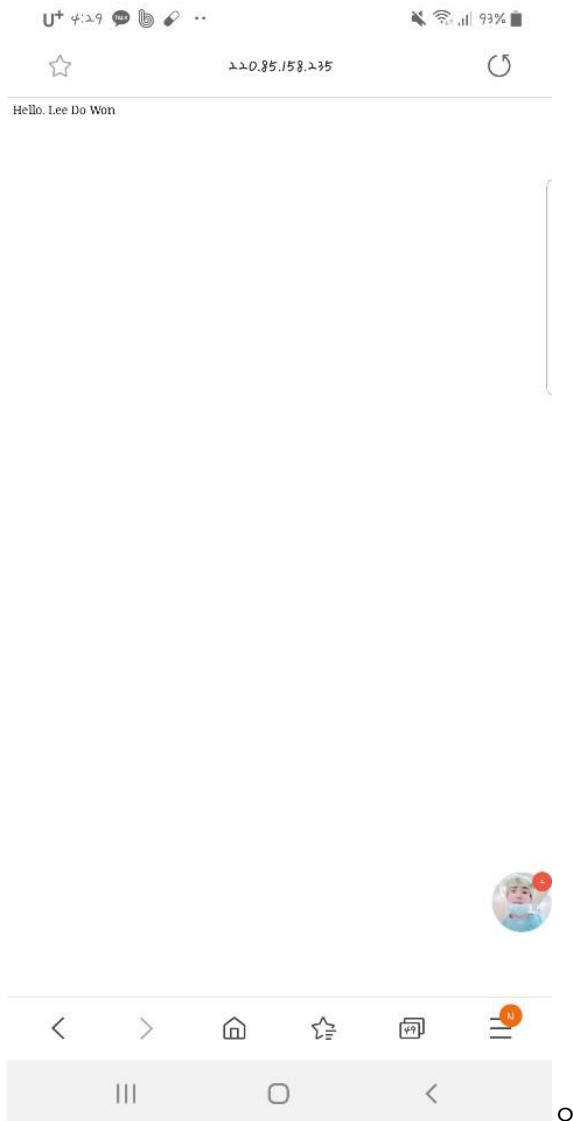
2) Untangle Port Forwarding

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

Static Routes Add Import Export						
	De...	Network	Netmask/Prefix	Next Hop	Edit	Delete
+	IP ...	192.168.70.0	24	192.168.80.2	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

3) IP Forwarding

- External DMZ 구역과 IPS Zone을 라우팅 해준다.



- 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.

```

Connecting to 192.168.70.22:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+J'.

Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

247 packages can be updated.
187 updates are security updates.

Last login: Sat Sep  7 07:20:07 2019 from 192.168.30.200
web@ubuntu:~$ ifconfig
ens33:  Link encap:Ethernet  HWaddr 00:0c:29:db:cb:44
        inet addr:192.168.70.22  Bcast:192.168.70.255  Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fedb:cb44/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:151 errors:0 dropped:0 overruns:0 frame:0
        TX packets:893 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:17835 (17.8 KB)  TX bytes:76814 (76.8 KB)

lo:      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:196 errors:0 dropped:0 overruns:0 frame:0
        TX packets:196 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:15170 (15.1 KB)  TX bytes:15170 (15.1 KB)

web@ubuntu:~$
  
```

```

C:\Windows\system32\cmd.exe

이더넷 어댑터 Bluetooth 네트워크 연결:

   미디어 상태 . . . . . : 미디어 연결 끊김
   연결별 DNS 접미사. . . . :

이더넷 어댑터 로컬 영역 연결:

   연결별 DNS 접미사. . . . :
   링크-로컬 IPv6 주소 . . . : fe80::300d:619b:b038:dcd4:11
   IPv4 주소 . . . . . : 192.168.30.200
   서브넷 마스크 . . . . . : 255.255.255.0
   기본 게이트웨이 . . . . . : 192.168.30.1

터널 어댑터 isatap.{648F471B-87D6-4457-8945-73090B9684AF}:

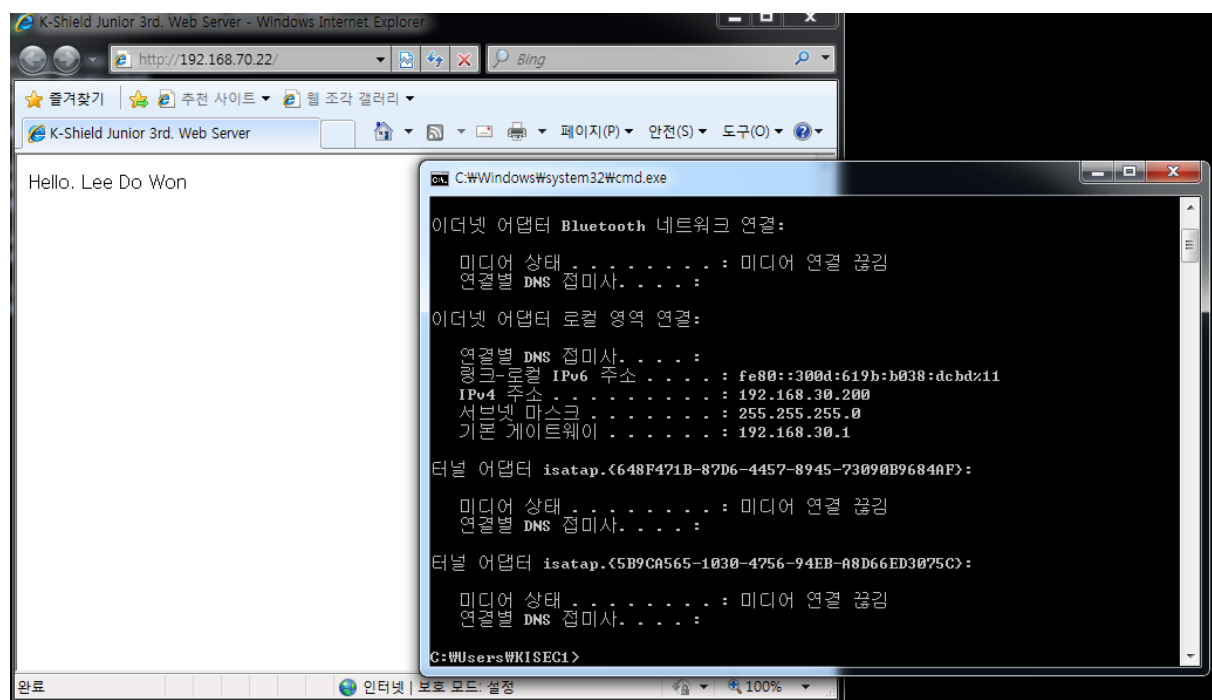
   미디어 상태 . . . . . : 미디어 연결 끊김
   연결별 DNS 접미사. . . . :

터널 어댑터 isatap.{5B9CA565-1030-4756-94EB-A8D66ED3075C}:

   미디어 상태 . . . . . : 미디어 연결 끊김
   연결별 DNS 접미사. . . . :

C:\Users\WKISEC1>
  
```

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          udp dpt:1514
ACCEPT     udp  --  192.168.30.200         anywhere
ACCEPT     udp  --  192.168.30.100        anywhere             udp dpt:1514

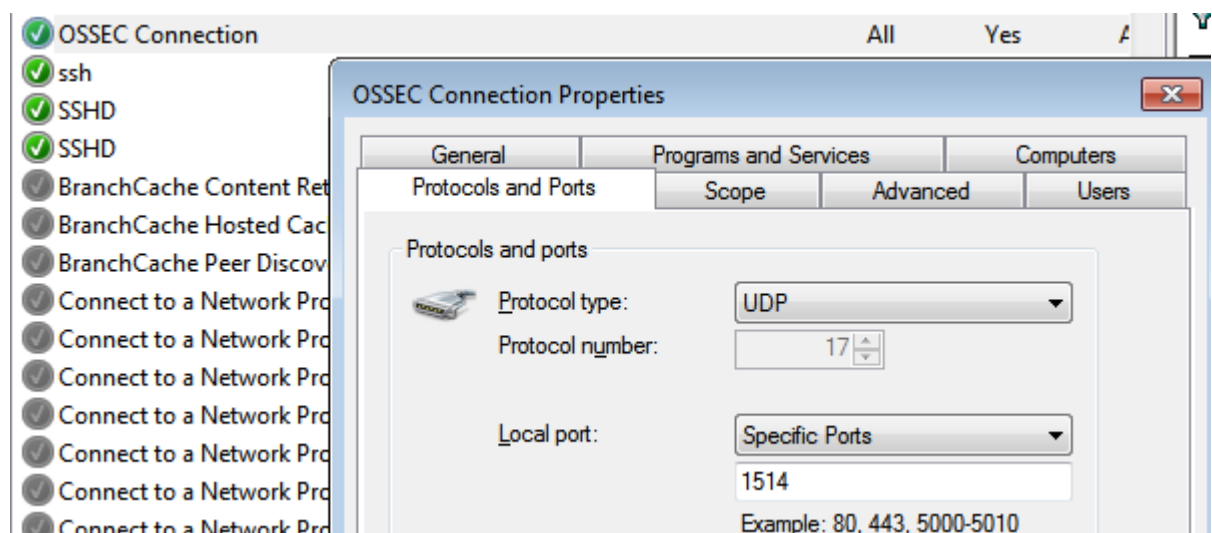
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

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

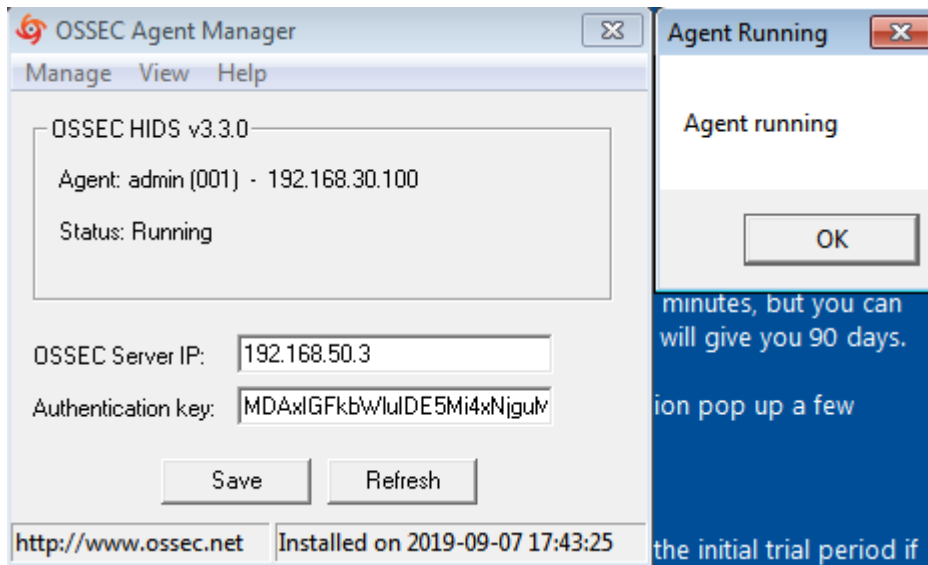
- OSSEC 서버에서 OSSEC Agent (Office 망 단말 전체를 대상) UDP 1514 포트 허용 (인바운드)
- 모든 아웃바운드 트래픽은 허용
- 개발자 PC와 관리자 PC로부터 UDP 1514 포트로의 접근을 허용

인바운드 규칙													
이름	그룹	프로토콜	사용	작업	다시 정의	프로그램	로컬 주소	원격 주소	프로토콜	로컬 포트	원격 포트	허용된 사용자	허용된 컴퓨터
✓ DRC		모두	예	허용	아니오	모두	모두	모두	TCP	3389	모두	모두	모두
✓ OSSEC Agent		모두	예	허용	아니오	모두	모두	모두	UDP	모두	모두	모두	모두

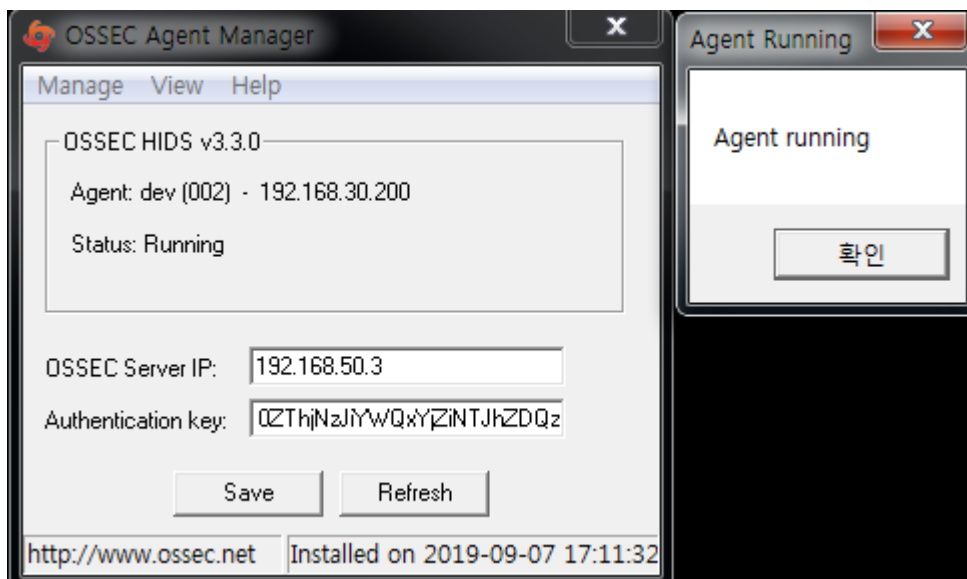
- 개발자 PC(Agent)에서의 UDP 1514 인바운드 규칙 생성



- 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.

```
root@ubuntu: /
root@ubuntu: /# service ssh status
ssh start/running, process 1247
root@ubuntu: /#
```

- 관리 서버에서 ssh 패키지 설치 후 가동 / 상태 확인

```
192.168.50.3
* Documentation: https://help.ubuntu.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Sat Sep  7 02:26:14 2019 from 192.168.30.100
ksil@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b7:d5:1d
          inet addr:192.168.50.3  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb7:d51d/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17861 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4919 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14511037 (14.5 MB)  TX bytes:637612 (637.6 KB)

C:\Administrator: C:\Windows\system32\cmd.exe
Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.30.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.30.1
```

- 관리자 PC에서 SSH 접속 화면

```
192.168.50.3
Xshell 6 (Build 0149)
Copyright (c) 2002 NetSarang Computer, Inc. All rights reserved.

Type 'help' to learn how to use Xshell prompt.
[C:\~]$

Connecting to 192.168.50.3:22...
Could not connect to '192.168.50.3' (port 22): Connection failed.

Type 'help' to learn how to use Xshell prompt.
[C:\~]$

C:\Windows\system32\cmd.exe

이더넷 어댑터 Bluetooth 네트워크 연결:

    미디어 상태 . . . . . : 미디어 연결 끊김
    연결별 DNS 접미사. . . . . :

이더넷 어댑터 로컬 영역 연결:

    연결별 DNS 접미사. . . . . :
    링크-로컬 IPv6 주소 . . . . . : fe80::300d:619b:b038:dcbd%11
    IPv4 주소 . . . . . : 192.168.30.200
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . : 192.168.30.1
```

- 개발자 PC에서 SSH 접속 불가능 화면

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

Options	QoS	Access Rules	UPnP	DNS & DHCP	Network Cards	Netflow	Dynamic Routing
Access Rules							
<div> <div>+</div> Add <div>↓ Import</div> <div>↑ Export</div> </div>							
Rule Id	Enable	IPv6	Description	Conditions	Block	Edit	Delete
1	<input type="checkbox"/>	<input type="checkbox"/>	Allow SSH	Destination Port ⇒ 22 • Protocol ⇒ TCP	<input type="checkbox"/>		
2	<input type="checkbox"/>	<input type="checkbox"/>	Allow HTTPS on WANs	Destination Port ⇒ 443 • Protocol ⇒ TCP • Source Interfac...	<input type="checkbox"/>		
3	<input type="checkbox"/>	<input type="checkbox"/>	Allow HTTPS on non-WANs	Destination Port ⇒ 443 • Protocol ⇒ TCP • Source Interfac...	<input type="checkbox"/>		
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Allow HTTPS on Admin(Office ...	Destination Port ⇒ 443 • Protocol ⇒ TCP, UDP • Source A...	<input type="checkbox"/>		
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Allow PING	Protocol ⇒ ICMP	<input type="checkbox"/>		
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Allow DNS on non-WANs	Destination Port ⇒ 53 • Protocol ⇒ TCP, UDP • Source Int...	<input type="checkbox"/>		
7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Allow DHCP on non-WANs	Destination Port ⇒ 67 • Protocol ⇒ UDP • Source Interface...	<input type="checkbox"/>		
8	<input type="checkbox"/>	<input type="checkbox"/>	Allow HTTP on non-WANs	Destination Port ⇒ 80 • Protocol ⇒ TCP • Source Interface...	<input type="checkbox"/>		
9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Allow HTTP on Admin(Office Z...	Destination Port ⇒ 80 • Protocol ⇒ TCP, UDP • Source Ad...	<input type="checkbox"/>		

Untangle – Config – Network – Advanced – Access Rules에서

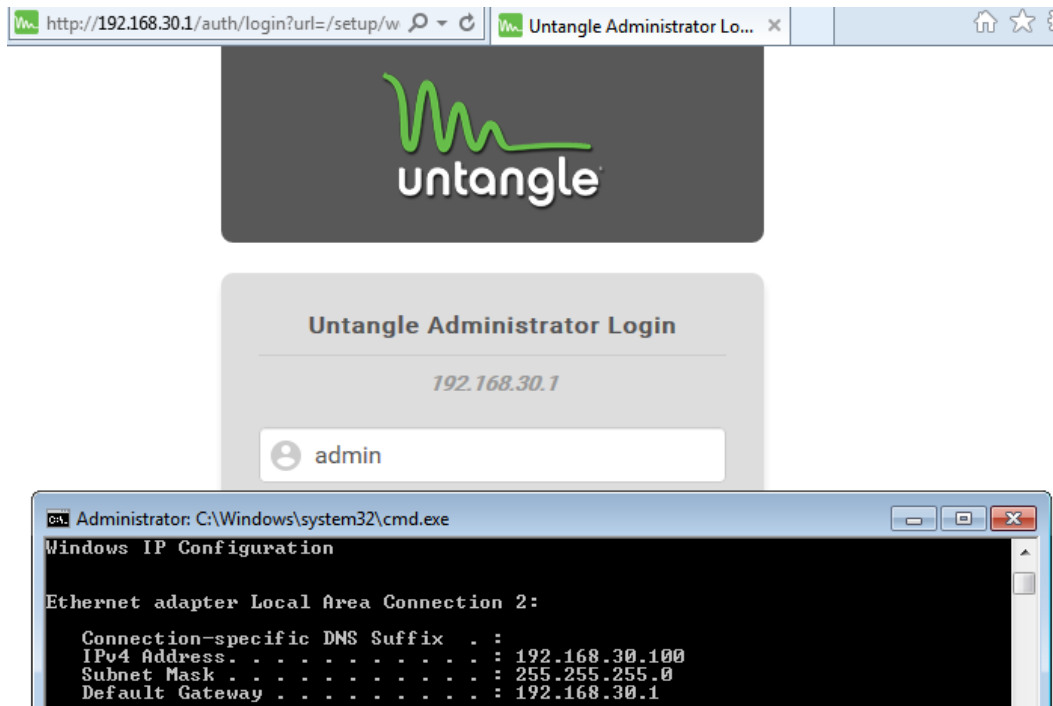
관리자 PC에서만 접근 가능하게 하기 위해 Allow HTTPS on non-WANs (Rule id : 3), Allow HTTP on non-WANs (Rule id : 8)을 비활성화하고, 새로운 정책을 2개 추가한다.

4) Allow HTTPS on Admin(Office Zone)

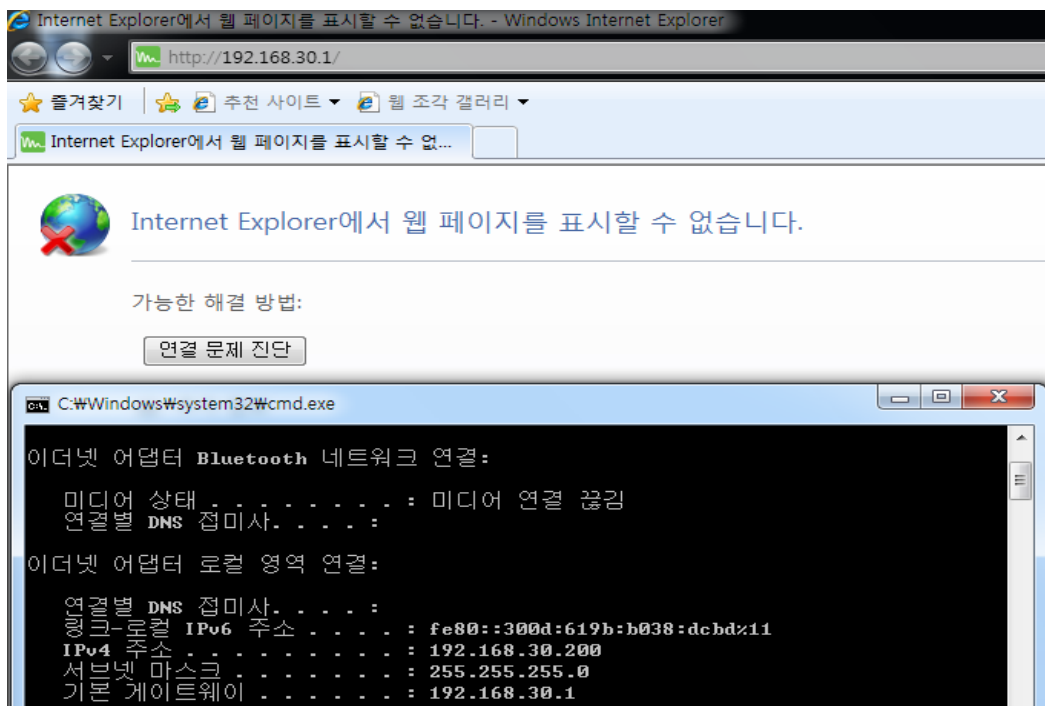
- 관리자에서의 HTTPS 접근을 허용하기 위해 정책을 설정
- Destination Port : 443 / Protocol : TCP, UDP / Source Address : 192.168.30.100

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

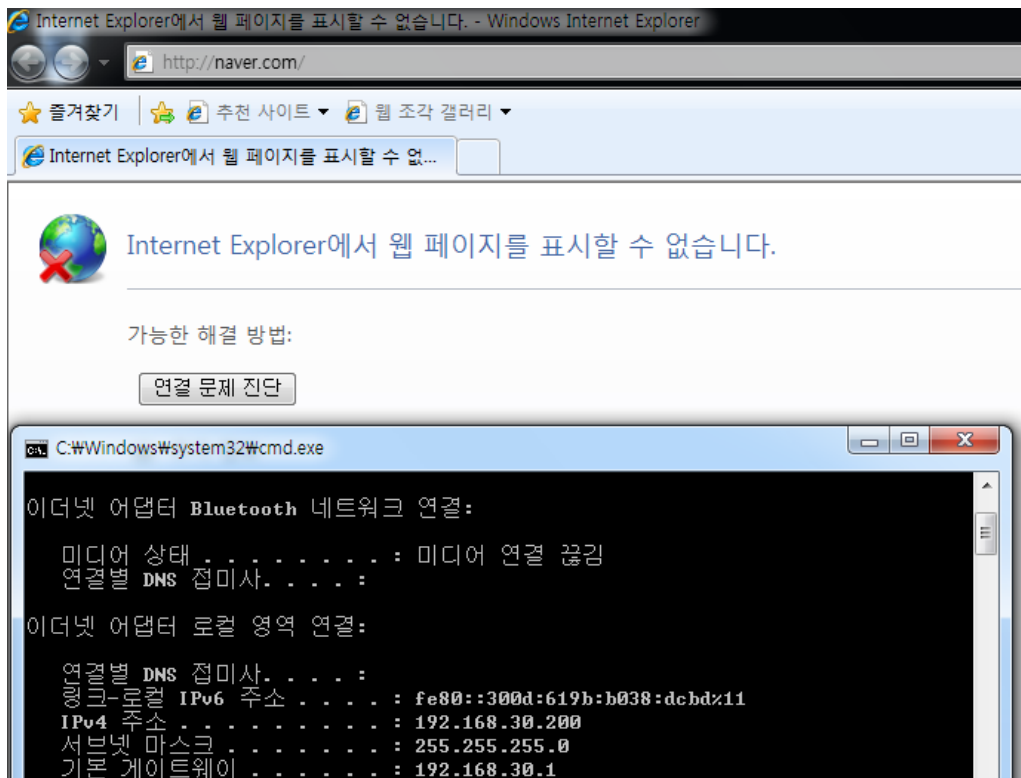


- 관리자 PC에서 방화벽 관리 페이지 HTTP 접속 완료

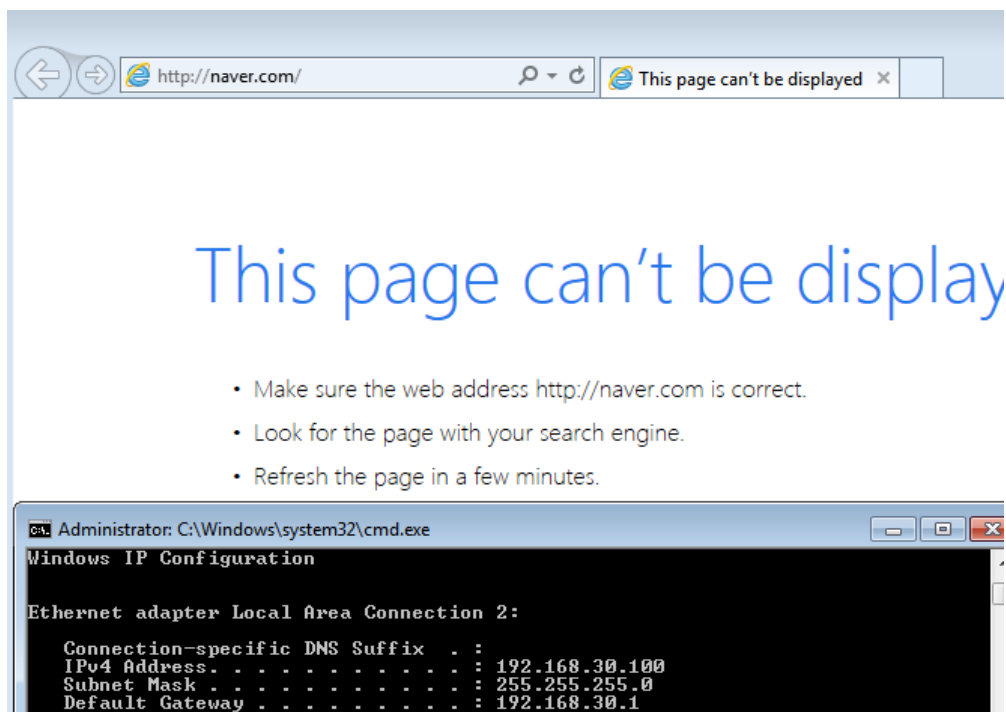


- 개발자 PC에서 방화벽 관리 페이지 접속 불가능

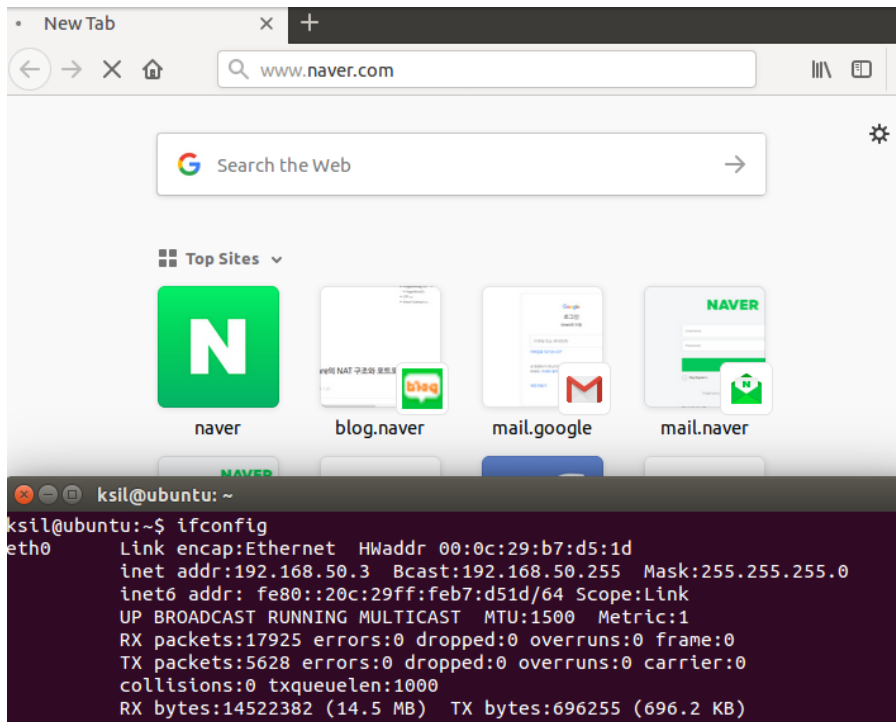
7] 내부의 있는 모든 망은 외부와의 인터넷이 불가능하다.



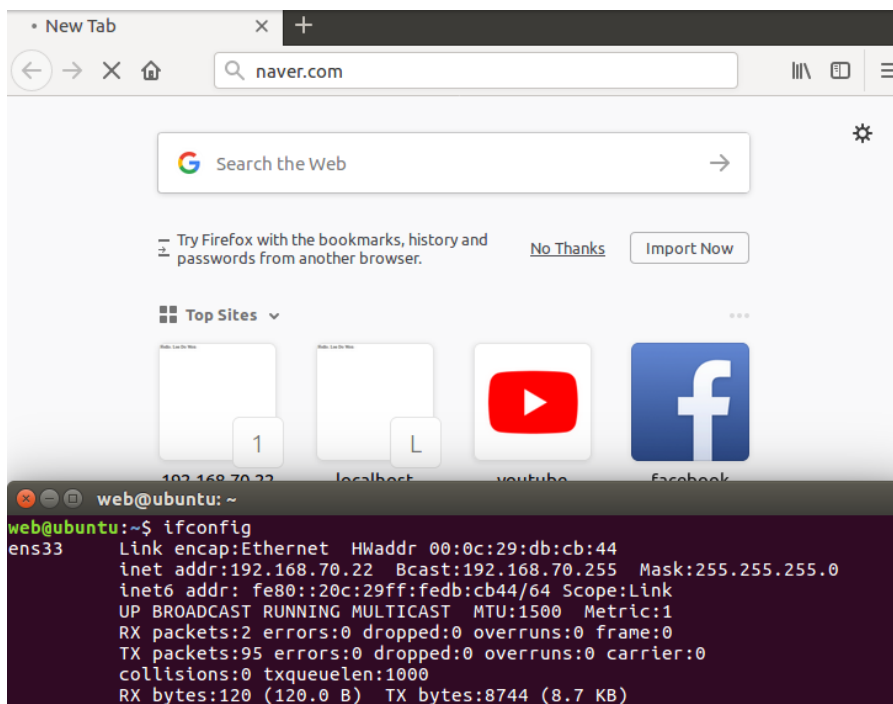
- Office Zone) 개발자 PC(192.168.30.200) 외부와의 인터넷 불가능



- 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