2021-04

「단기과제」

VMware ESXi와 오픈소스를 활용한 가상 보안 인프라 환경 구축

정보보호 진단관리 과정

주대원

목 차

표 목차

그림 목차

1 개요

1.1 주제

단기 과제의 주제는 오픈소스를 활용한 가상 보안 인프라 환경 구축으로 본 문서에서는 VMware ESXi를 활용하여 구축을 진행한다.

1.2 시나리오

OOO 기업에서는 사내 보안 인프라를 구축하고 고객들을 위한 웹서비스를 운영할 방침이다. 운영을 위한 서버는 서비스 기준으로 내부 직원 PC 관리를 위한 내부망과 외부 고객을 위한 웹 서비스가 운영되는 웹 서버 또는 데이터베이스 등이 위치할 DMZ 망을 별도로 구성한다.

직원 PC와 내부망은 외부와의 통신(인터넷)을 단절하여 사전에 외부로 유출할 수 있는 가능성을 차단하고, 직원 PC들의 위협 탐지를 위해 HIDS의 에이전트 방식으로 설치하여 이상 여부 확인 서버를 구축한 뒤 위협 모니터링하고자 한다.

OOO 기업은 외부의 웹사이트를 개방하여 고객 일부를 위한 웹서비스 제공하고 이 웹서비스는 개발자만 접근할 수 있도록 통제하여 개발자가 업무망에서만 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, 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 자리매김해야 한다.

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

그림 1-1 가상 시나리오

인프라 구축을 위한 시나리오는 그림 1-1과 같으며 이를 기반으로 하여 인프라를 구성한다.

1.3 요구사항

1.3.1 인프라 구성

1) 네트워크 통신 장비(vSwitch 등)를 제외한 이미지 총 6개 설치
-> 방화벽, IPS, 개발자 PC, 관리자 PC, 웹 서버, HIDS 관리 서버(Endpoint Management Server)
2) 통신망은 외부 인터넷, DMZ, 내부망(Internal Zone), 오피스망(Office Zone)으로 구분
3) 각 통신은 최소한의 원칙에 따라 구성되어야 하며, 필요하지 않은 보안 정책은 차단하여 접근 통제를 수행
4) HIDS 관리 서버는 보안 솔루션인 Wazuh(HIDS 솔루션)의 서버로 활용하며, Agent는 개발자PC와 관리자PC에서 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, Wazuh는 리눅스 계열, 전직원 PC는 윈도우 계열로 고정

그림 1-2 인프라 구성 목록

구성해야 할 인프라 환경에 대한 요구사항은 그림 1-2와 같다.

1.3.2 접근 통제 규정

1) 방화벽의 모든 접근 통제는 화이트리스트 기반(All Deny)으로 적용함
2) 웹 서버는 외부(구축되는 호스트 PC의 외의 다른 장비(예: 휴대폰, 노트북 등))에서 HTTP 접속이 가능해야 함
3) 웹 서버는 오피스망의 개발자 PC만 HTTP 포트와 SSH 포트 접속이 가능해야 함
4) HIDS 관리 서버는 에이전트 정책 관리를 위해 오피스망 단말 전체를 대상으로 필요한 포트만 활성화함
5) HIDS 관리 서버의 수정과 서비스 관리를 위하여 관리자PC에서만 SSH 접속 가능하도록 설정함
6) 방화벽 접근은 오직 관리자 PC에서만 접근 가능하며, 관련 설정은 초기 설정 외에 모두 관리자 PC에서만 수행함
7) 내부의 있는 모든 망은 외부와의 인터넷이 불가능함

그림 1-3 접근 통제 규정 목록

방화벽에 적용해야 할 접근 통제 규정 목록은 그림 1-3과 같다. 방화벽 룰은 화이트리스트 기반으로 작성할 예정이며, 규정에 따라 각 단말에 룰을 적용한다.

2 인프라 구축

2.1 VMware ESXi

그림 2-1 ESXi

VMware ESXi는 하드웨어에 직접 설치하는 가상화 프로그램으로 하드웨어 바로 위에서 동작하기 때문에 하드웨어의 리소스를 전부 사용할 수 있다.

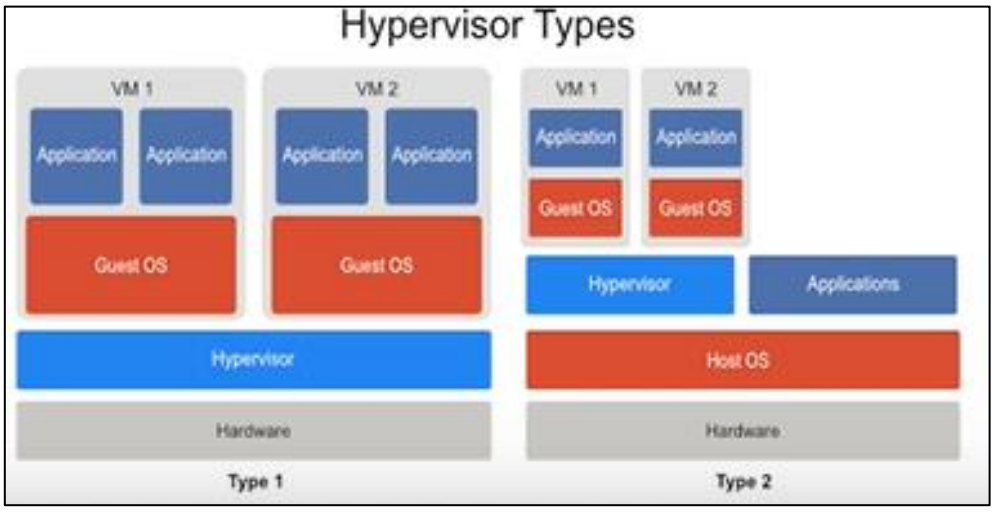


그림 2-2 하이퍼바이저 유형[1]

VMware Workstation과 ESXi의 가상화 방식은 Type1, Type2로 나눌 수 있다. Type1은 하드웨어 위에 바로 하이퍼바이저를 설치하는 ESXi에 해당하고 Type2는 하드웨어에 운영체제가 설치된 상태로 하이퍼바이저가 올라가는 VMware Workstation에 해당한다.

[1] 출처: https://www.vembu.com/blog/top-11-microsoft-hyper-v-terminologies-you-need-to-know

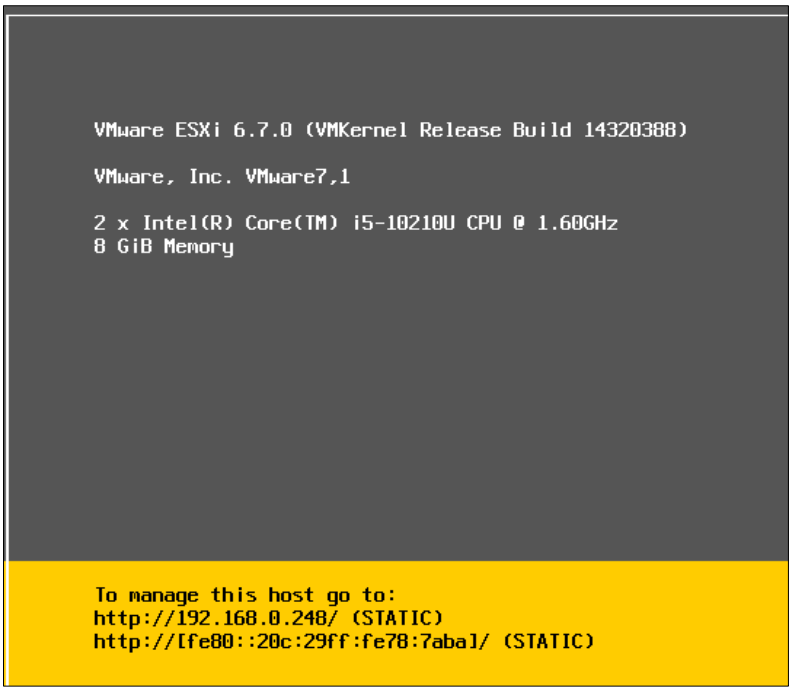


그림 2-3 ESXi 실행

VMware Workstation에 ESXi 6.7 버전을 설치하고 네트워크를 NAT(VMnet8)로 설정한 뒤 실행한다. ESXi의 IP 주소는 192.168.0.248이다.

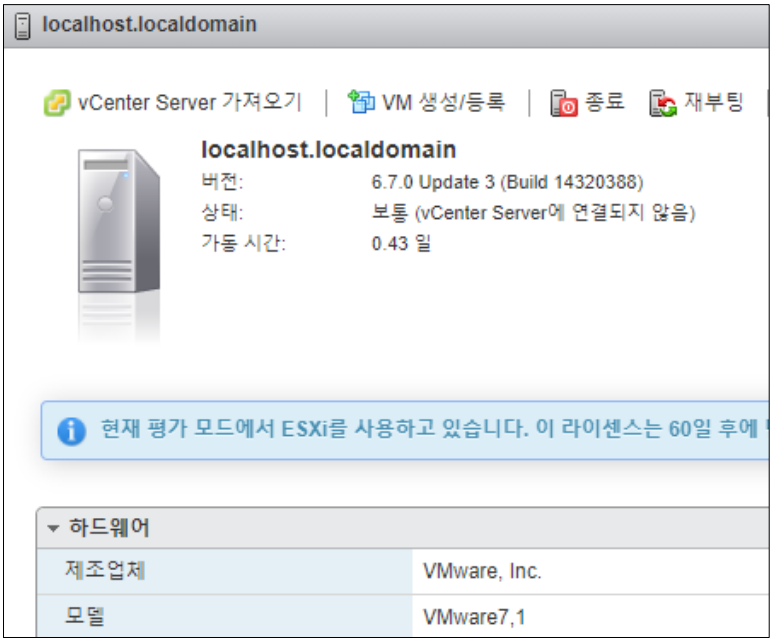


그림 2-4 http://192.168.0.248

해당 IP 주소를 통해 가상 시스템, 스토리지, 네트워크 설정을 할 수 있는 웹 페이지에 접속한다.

2.2 인프라

2.2.1 개요

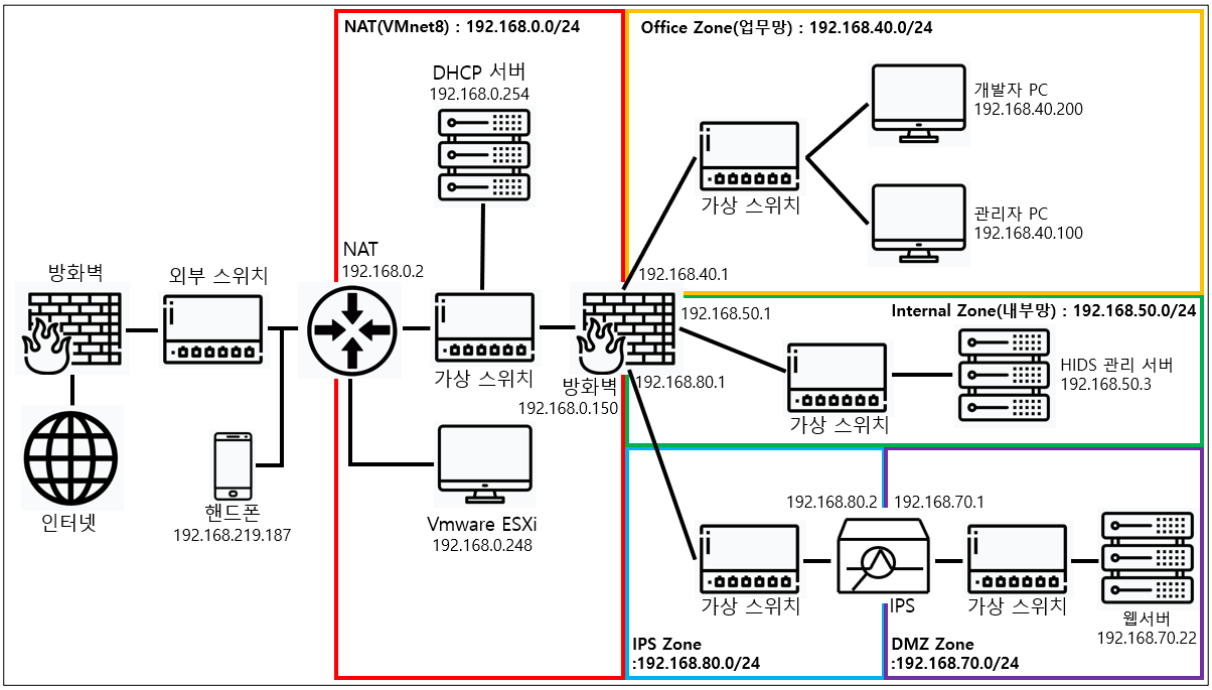


그림 2-5 인프라 구성도

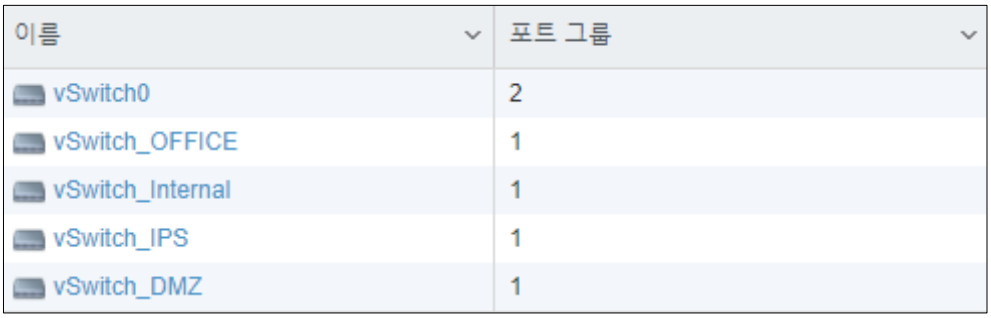
구축할 인프라 구성도는 그림 2-5와 같다. 설치해야 할 가상 시스템은 6개이고 가상 스위치와 포트 그룹은 각각 4개이다.

No	가상 이미지	사용 구분	버전	RAM	네트워크 위치	VMnet IP대역	IP주소
1	Firewall	방화벽	Debian (Untangle)	1GB	WAN	192.168.0.0/24	192.168.0.150
2					Office Zone	192.168.40.0/24	192.168.40.1
3					Internal Zone	192.168.50.0/24	192.168.50.1
4					IPS Zone	192.168.80.0/24	192.168.80.1
5	admin_PC	PC	Windows 7	1GB	Office Zone	192.168.40.0/24	192.168.40.100
6	developer_PC	PC	Windows 7	1GB	Office Zone	192.168.40.0/24	192.168.40.200
7	IPS	IPS	CentOS 6.9 (suricata)	1GB	IPS Zone	192.168.80.0/24	192.168.80.2
8					DMZ Zone	192.168.70.0/24	192.168.70.1
9	Web_Server	Server	Windows 7	1GB	DMZ Zone	192.168.70.0/24	192.168.70.22
10	HIDS_Server	Server	CentOS 8	4GB	Internal Zone	192.168.50.0/24	192.168.50.3

표 2-1 가상 시스템 정보

인프라 구축에 사용할 가상 시스템의 상세 정보는 표 2-1과 같다.

2.2.2 네트워크 설정



이름	포트 그룹
vSwitch0	2
vSwitch_OFFICE	1
vSwitch_Internal	1
vSwitch_IPS	1
vSwitch_DMZ	1

그림 2-6 가상 스위치 목록

가상 시스템 간 연결을 위해 사용할 vSwitch_OFFICE, Internal, IPS, DMZ 스위치를 생성한다.

이름	활성 포트	VLAN ID	유형	vSwitch
VM Network	0	0	표준 포트 그룹	vSwitch0
Management Network	1	0	표준 포트 그룹	vSwitch0
P_Office	0	0	표준 포트 그룹	vSwitch_OFFICE
P_Internal	0	0	표준 포트 그룹	vSwitch_Internal
P_IPS	1	0	표준 포트 그룹	vSwitch_IPS
P_DMZ	1	0	표준 포트 그룹	vSwitch_DMZ

그림 2-7 포트 그룹 목록

방화벽은 VM network 포트를 통해 표준 스위치(vSwitch0)와 연결하여 외부 통신이 가능하게 한다. 그 외 가상 시스템은 네트워크망에 따라 적절한 포트와 스위치에 연결한다.

가상 스위치	포트 그룹	연결된 가상 시스템
vSwitch	VM Network	Firewall
vSwitch_OFFICE	P_Office	Firewall
		admin_PC
		developer_PC
vSwitch_Internal	P_Internal	Firewall
		HIDS_Management_Server
vSwitch_IPS	P_IPS	Firewall
		IPS
vSwitch_DMZ	P_DMZ	IPS
		Web_Server

표 2-2 네트워크 정보

인프라 구축에 사용한 네트워크 상세 정보는 표 2-2와 같다.

2.2.3 가상 시스템

1) 방화벽

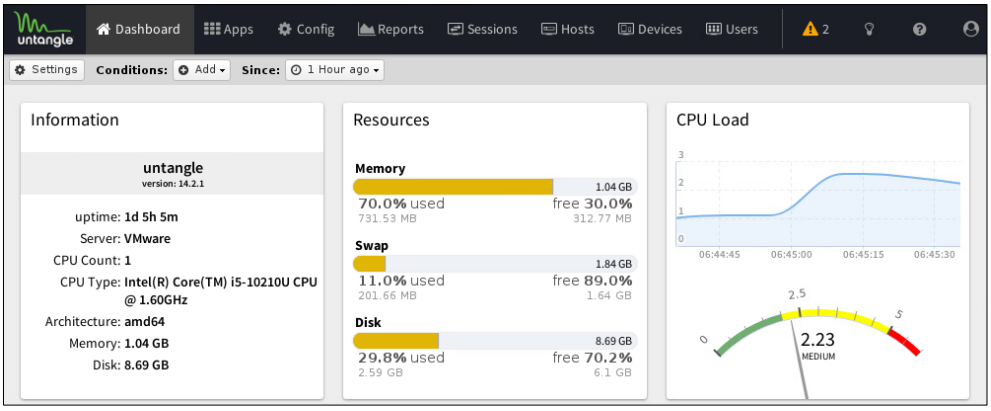


그림 2-8 Untangle

방화벽은 네트워크 관리 소프트웨어를 제공하는 Untangle을 이용하여 구축했다. Untangle은 오픈 소스로 방화벽, 안티 스팸, 안티 바이러스, OpenVPN 등의 기능을 제공하는 UTM(Unified Threat Management) 장비이다.

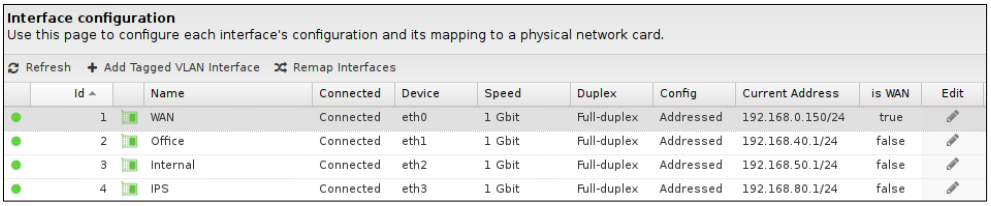


그림 2-9 네트워크 설정

외부 통신을 위한 WAN, 업무망 통신을 위한 Office, 내부망 통신을 위한 Internal, IPS망 통신을 위한 IPS 인터페이스를 설정한다. 접근 통제 규정에 의해 외부에서 웹 서버 접속이 가능하도록 몇 가지 설정을 추가한다.

그림 2-10 인바운드 규칙

웹 서버 접속 시 4000번 포트를 사용하기 위해 호스트PC 방화벽 인바운드 규칙에 4000번 포트 허용 룰을 추가한다.

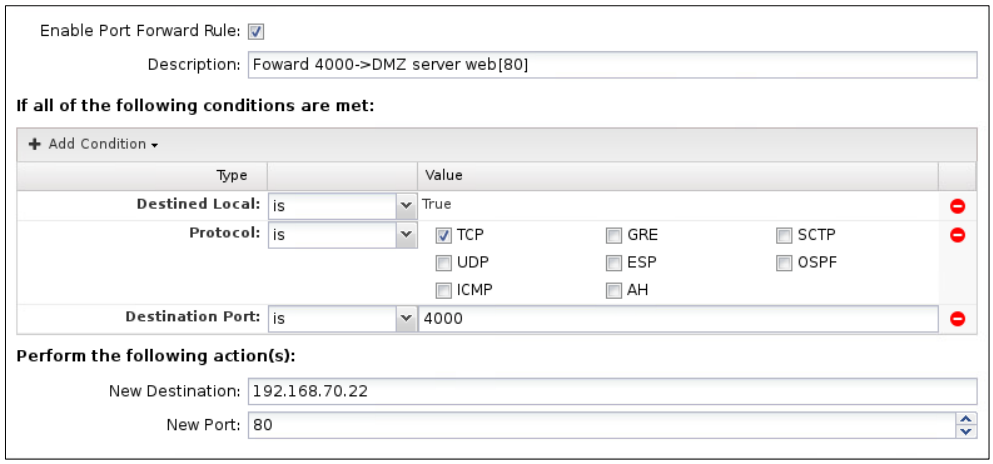


그림 2-11 포트 포워딩 룰

방화벽(Untangle)에 호스트PC에서 DMZ망에 있는 웹 서버(192.168.70.22)에 접근할 수 있도록 포트 포워딩 룰을 추가한다. 해당 룰을 통해 호스트는 PC는 방화벽 IP 주소:포트번호(192.168.0.150:4000)을 입력하여 웹 서버에 접근할 수 있다.

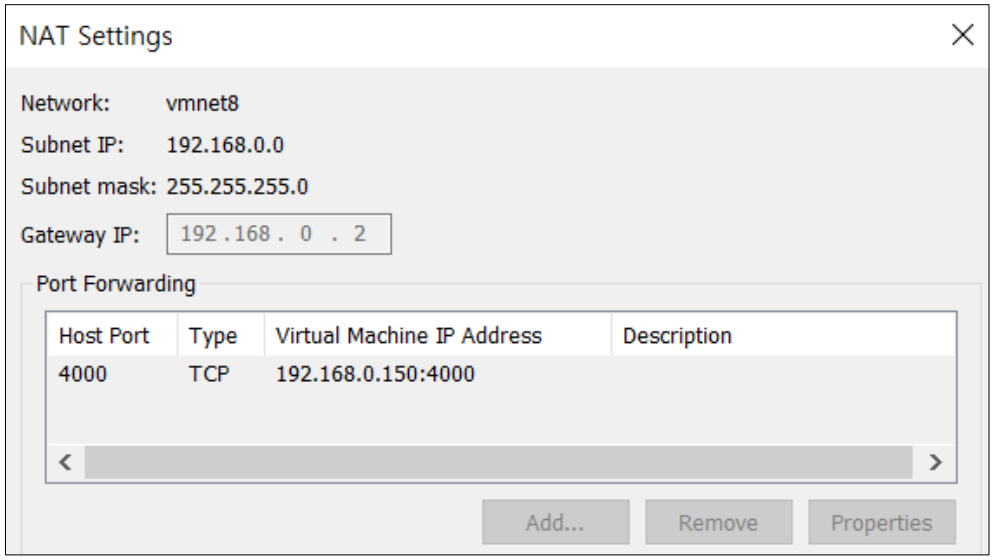


그림 2-12 VMware 포트 포워딩

접근 통제 규정에 따르면 외부 단말에서 웹 서버에 접속할 수 있어야 한다. VMware 포트 포워딩 설정 후 외부 단말에서 호스트 PC IP주소:4000을 입력하면 그림 2-11과 그림 2-12 룰에 의해 웹 서버 접속이 가능하다.

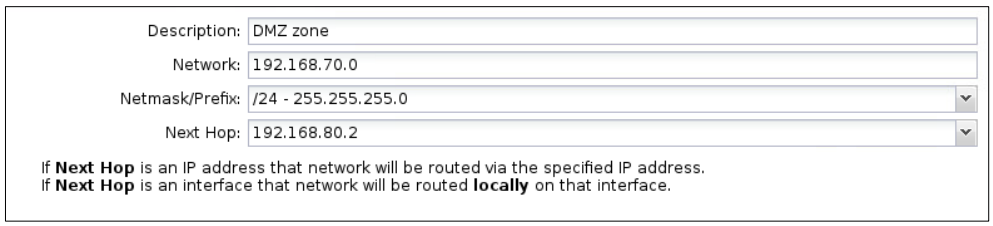


그림 2-13 라우팅 룰

DMZ망 네트워크(192.168.70.0)가 IPS(192.168.80.2)에 도달할 수 있도록 라우팅을 설정한다.

2) IPS(Suricata)

그림 2-14 Suricata

IPS는 IDS/IPS 기능을 제공하는 Suricata를 이용하여 구축했다. Suricata는 오픈소스로 실시간 침임 탐지(IDS), 인라인 침입 방지(IPS), 네트워크 보안 모니터링(NSM) 등의 기능을 제공하며 네트워크 래픽 검사 및 탐지가 가능하다.

```
[root@ips ~]# iptables -nvL
Chain INPUT (policy ACCEPT 767 packets, 59076 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
22750   30M NFQUEUE    all  --  *      *       0.0.0.0/0            0.0.0.0/0           NFQUEUE num
0

Chain OUTPUT (policy ACCEPT 48 packets, 2964 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

그림 2-15 iptables 룰

Suricata는 패킷 큐(대기열)에 대한 접근 권한을 주는 NFQUEUE 라이브러리를 이용한다. iptables 에 NFQUEUE 설정을 추가하여 Suricata가 트래픽을 제어할 수 있게 한다.

```
[root@ips ~]# suricata -c /usr/local/etc/suricata/suricata.yaml -q 0
16/4/2021 -- 10:17:40 - <Notice> - This is Suricata version 4.0.5 RELEASE
16/4/2021 -- 10:17:50 - <Notice> - all 3 packet processing threads, 4 management threads initialized
, engine started.
```

그림 2-16 Suricata 실행

`suricata -c /usr/local/etc/suricata/suricata.yaml -q 0` 명령어를 이용해 Suricata를 실행한다.

3) HIDS 관리 서버

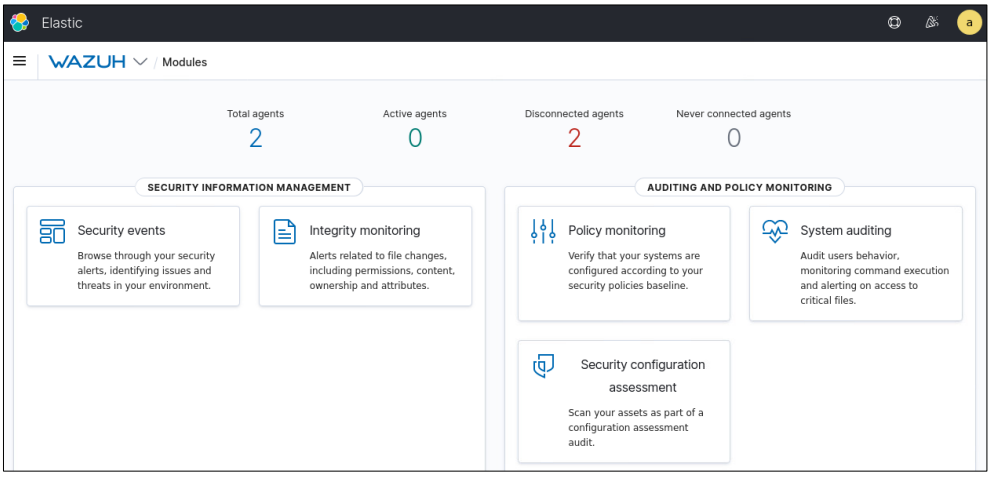


그림 2-17 WAZUH

HIDS(Host-based Intrusion Detection System)는 Wazuh를 이용하여 구축했다. Wazuh는 오픈소스 IDS/IPS인 ossec을 기반으로 한 솔루션으로 로그 모니터링, 침입탐지, 안티 멀웨어/루트킷 탐지 등의 기능을 제공한다.

4) 웹서버

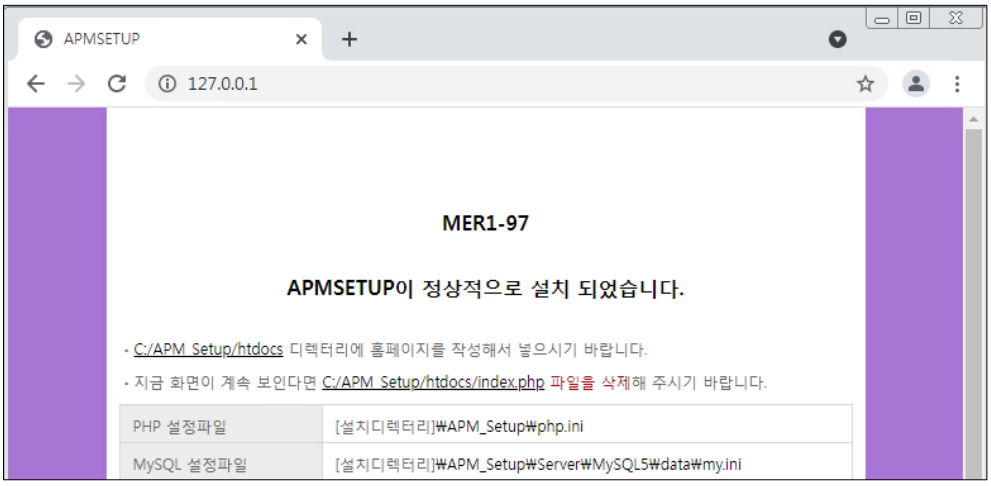


그림 2-18 APMSetup

웹서버는 Winodws7에 APMSetup을 이용하여 구축했다. APM은 웹 서버 구현을 위해 사용하는 Apache, PHP, MySQL을 통칭하며 APMSetup을 통해 세 가지를 한 번에 설치, 연동 및 관리할 수 있다.

5) 관리자PC, 개발자PC

관리자PC와 개발자 PC는 Windows7을 이용하여 구축하였다.

3 접근 통제 규정

3.1 화이트리스트 기반 방화벽 룰

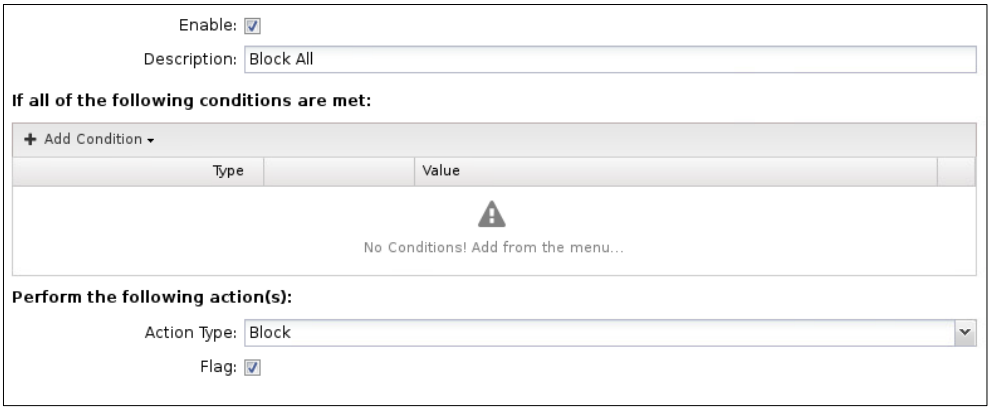


그림 3-1 Block All

방화벽의 모든 접근 통제는 화이트리스트 기반으로 이루어져야 한다. 허용하지 않은 모든 접근을 차단하도록 그림 3-1과 같이 방화벽 룰을 설정한다. 룰의 id는 100007이다.

3.2 외부에서 웹서버 접속

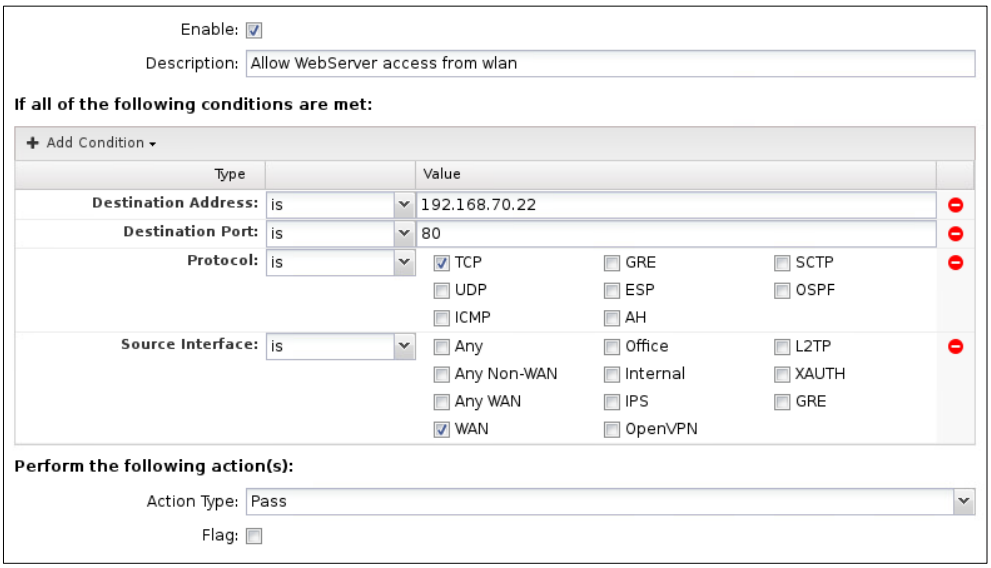


그림 3-2 Allow Webserver access from wlan

외부(Wlan)에서 웹서버 접근이 가능하도록 그림 3-2와 같이 방화벽 룰을 설정한다. 룰의 id는 100001이다.

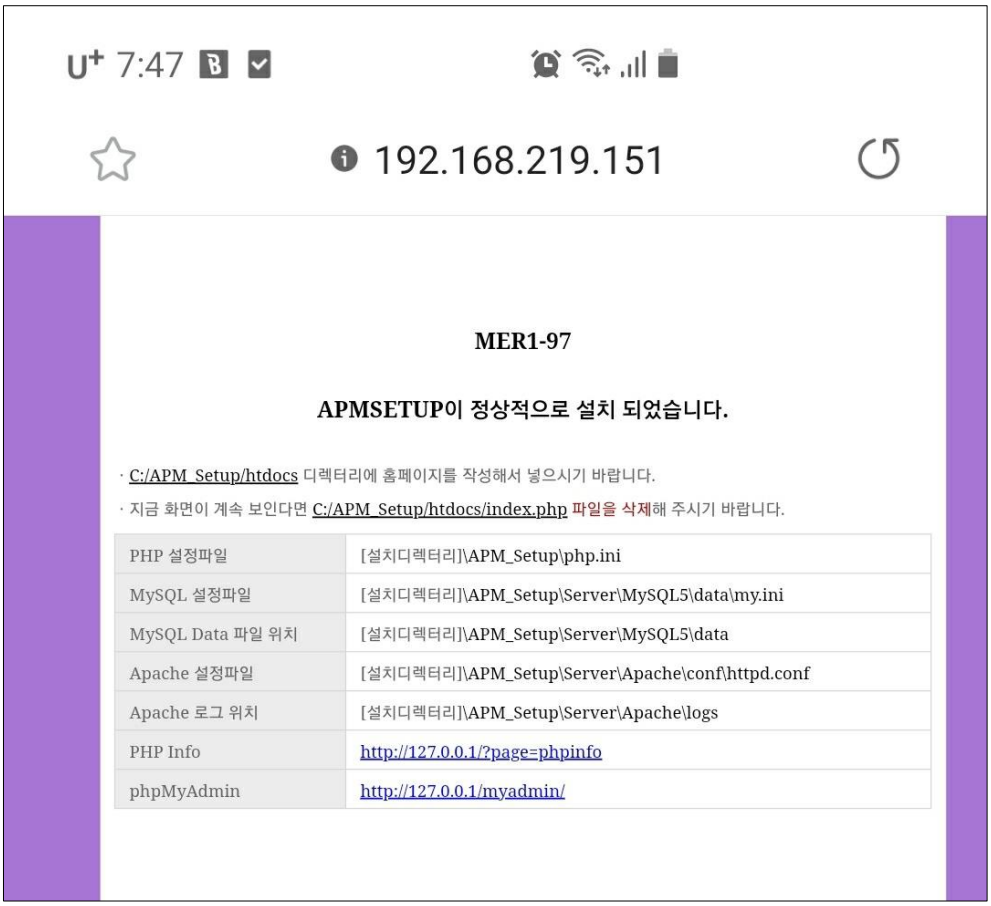


그림 3-3 웹서버 접속

핸드폰 웹 브라우저에 호스트PC의 IP주소와 4000번 포트를 입력한 결과 DMZ망에 있는 웹서버에 성공적으로 접속했다.

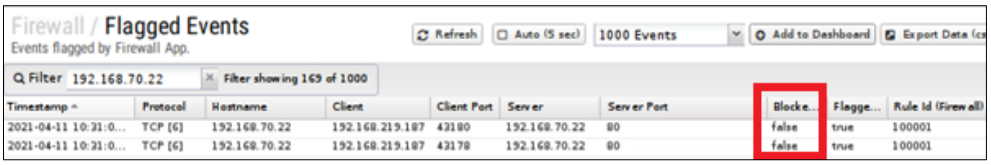


그림 3-4 Flagged Events

핸드폰(192.168.219.187)에서 웹서버(192.168.70.22)로 접속할 때 100001 룰에 의해 통과되었다.

3.3 개발자PC에서 웹서버 HTTP, SSH 접속

웹서버는 Office망의 개발자PC만 HTTP, SSH 포트 접속이 가능해야 한다.

1) HTTP 접속

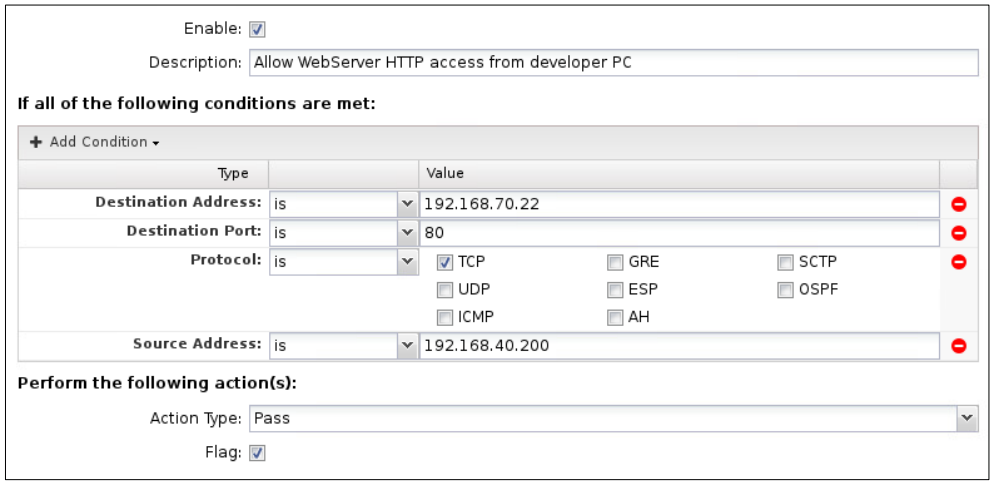


그림 3-5 Allow Webserver HTTP access from developer PC

개발자PC(192.168.40.200)에서 웹서버(192.168.70.22) HTTP 접근이 가능하도록 그림 3-5와 같이 방화벽 룰을 설정한다. 룰의 id는 100002이다.

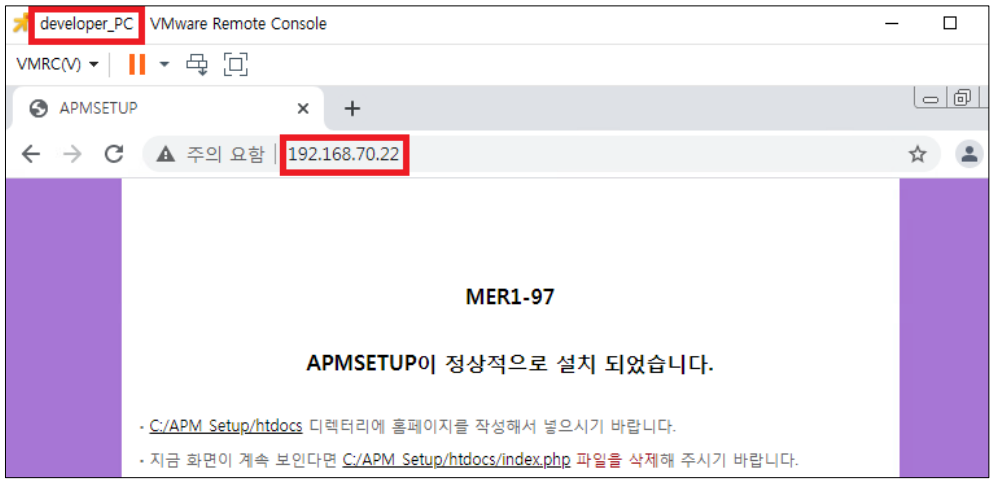


그림 3-6 웹서버 접속 성공

개발자PC에서 웹서버 IP 주소를 입력하면 웹서버 접근이 가능하다.

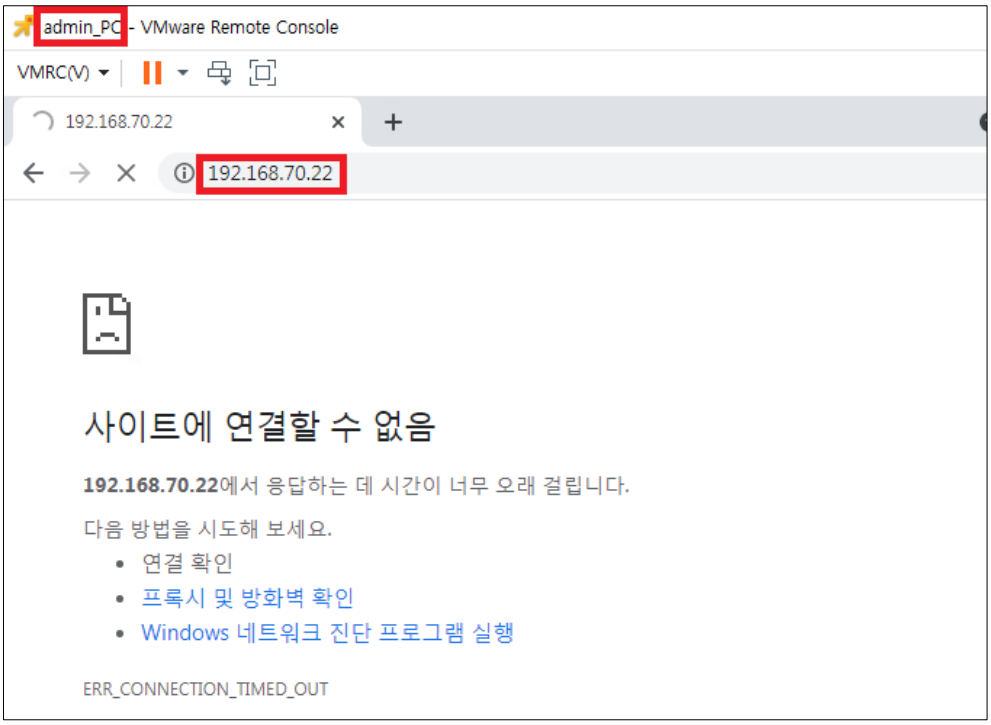


그림 3-7 웹서버 접속 실패

관리자PC에서 웹서버 IP 주소를 입력하면 웹서버 접근이 불가능하다.

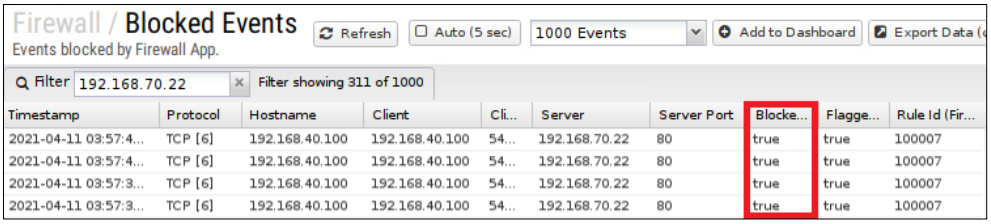


그림 3-8 Flagged Events

관리자PC(192.168.40.100)에서 웹서버(192.168.70.22)로 접속할 때 방화벽 100007 룰에 의해 거부되었다.

2) SSH 접속

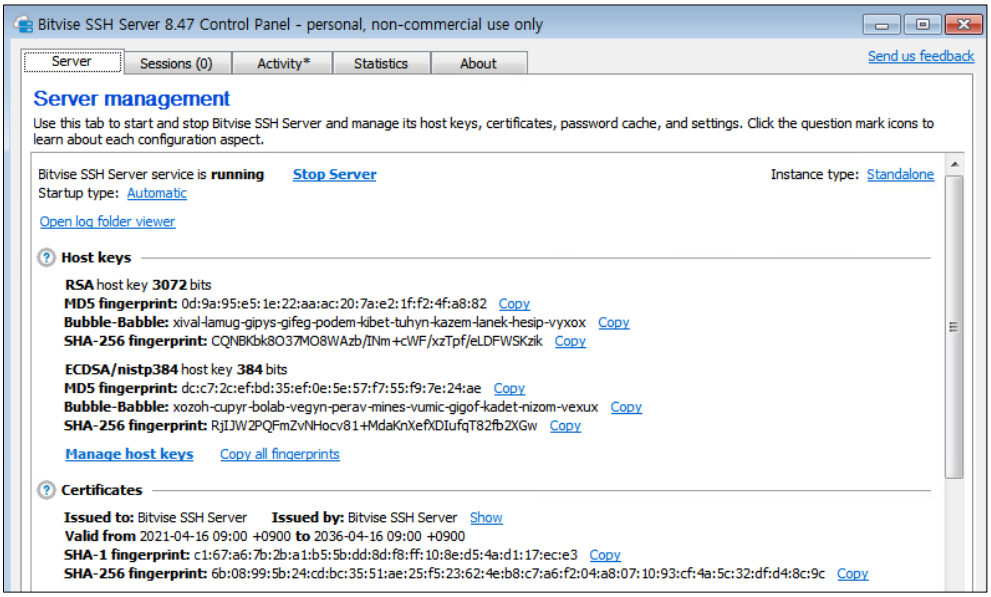


그림 3-9 Bitvise SSH Server

Windows 환경에서 SSH 서버 환경을 구축하기 위해 Bitvise SSH Server를 이용한다.

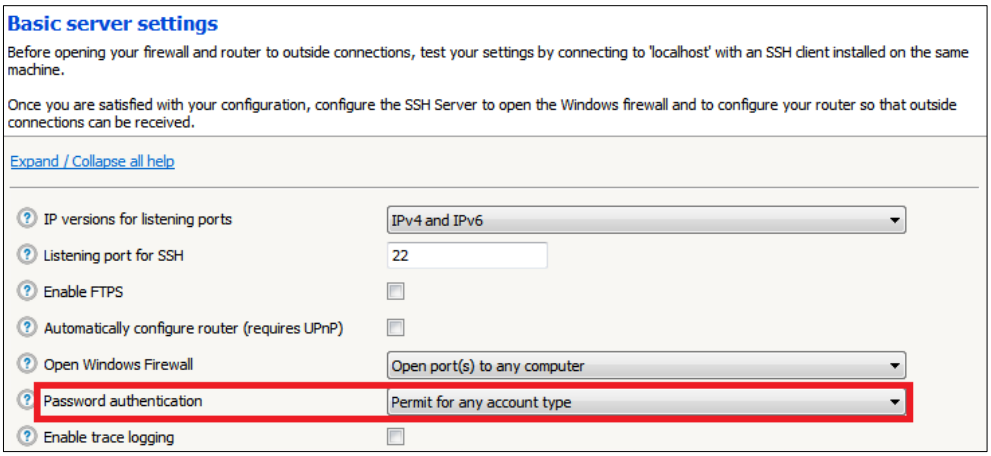


그림 3-10 인증 허용

어떤 계정이든 패스워드 인증을 할 수 있도록 Password authentication 설정을 한다.

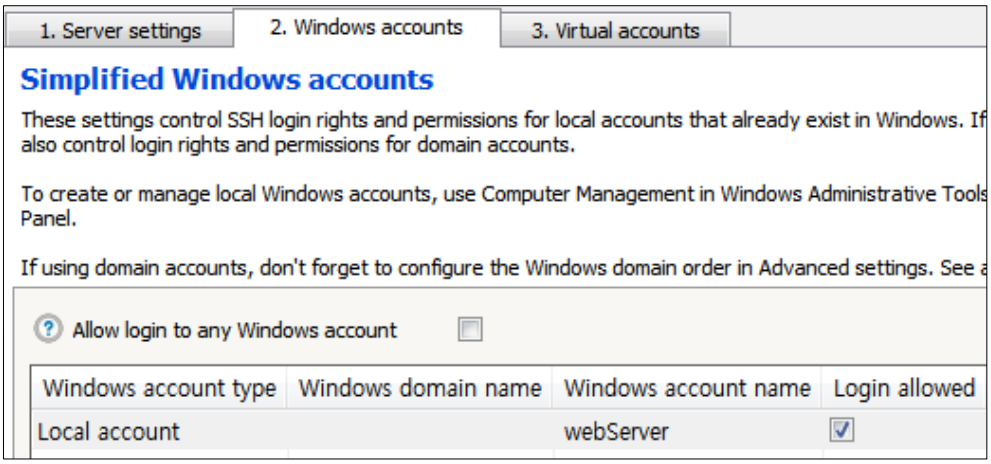


그림 3-11 로컬 계정 설정

SSH 로그인 시 계정 이름을 이용해 접속을 허용하도록 Windows 계정을 추가한다.

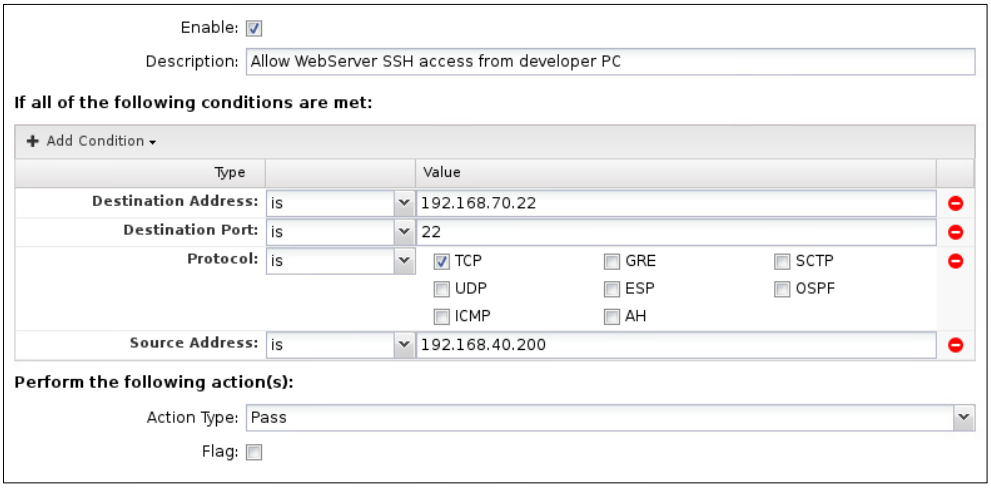


그림 3-12 Allow Webserver SSH access from developer PC

개발자PC(192.168.40.200)에서 웹서버(192.168.70.22) SSH 접근이 가능하도록 그림 3-12와 같이 방화벽 룰을 설정한다. 룰의 id는 100003이다.

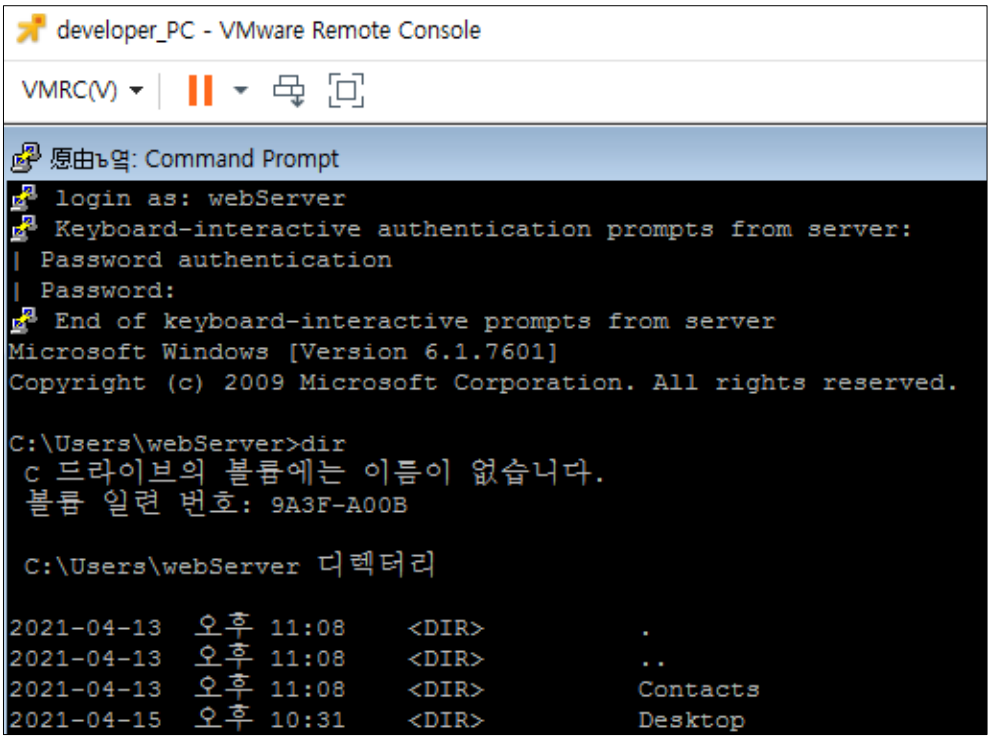


그림 3-13 SSH 접속 성공

개발자PC에서 SSH를 이용하여 웹서버 접근이 가능하다.

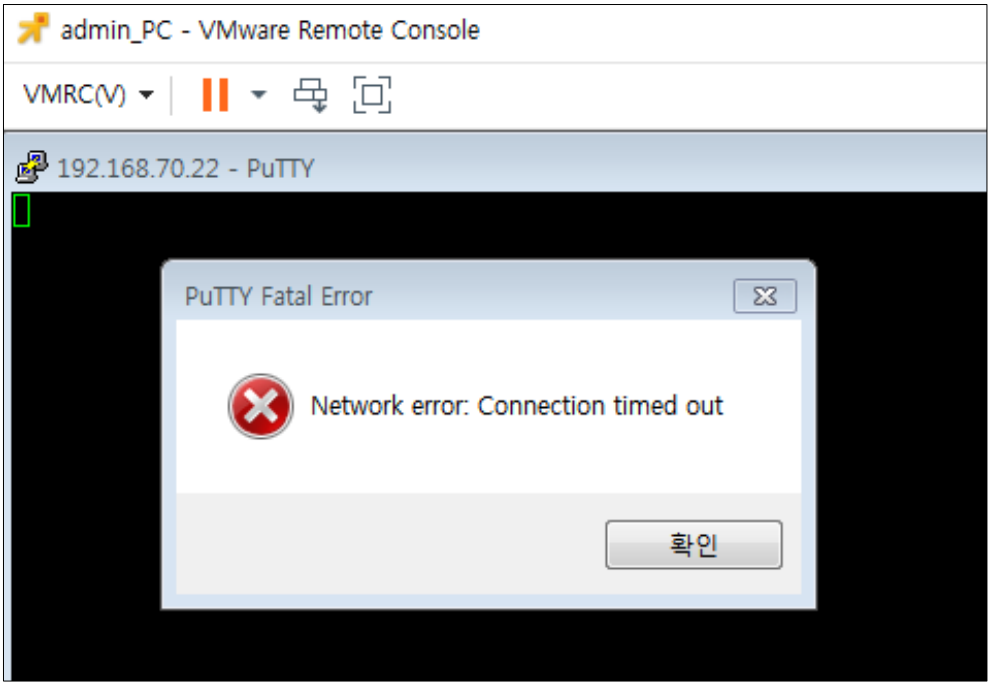


그림 3-14 SSH 접속 실패

관리자PC에서 SSH를 이용하여 웹서버 접근이 불가능하다.

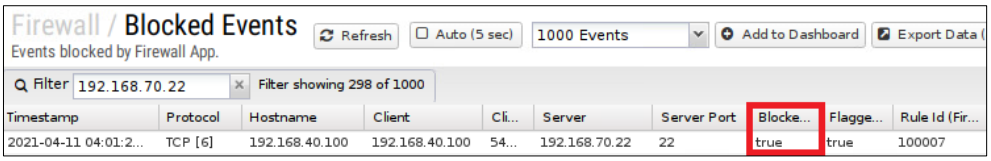


그림 3-15 Flagged Events

관리자PC(192.168.40.100)에서 웹서버(192.168.70.22)로 SSH 접속할 때 방화벽 100007 룰에 의해 거부되었다.

3.4 HIDS 관리 서버와 에이전트 설정

Wazuh 관리 서버에서 에이전트를 등록한 후 Office망에 존재하는 단말에 Wazuh 에이전트 프로그램을 설치한다.

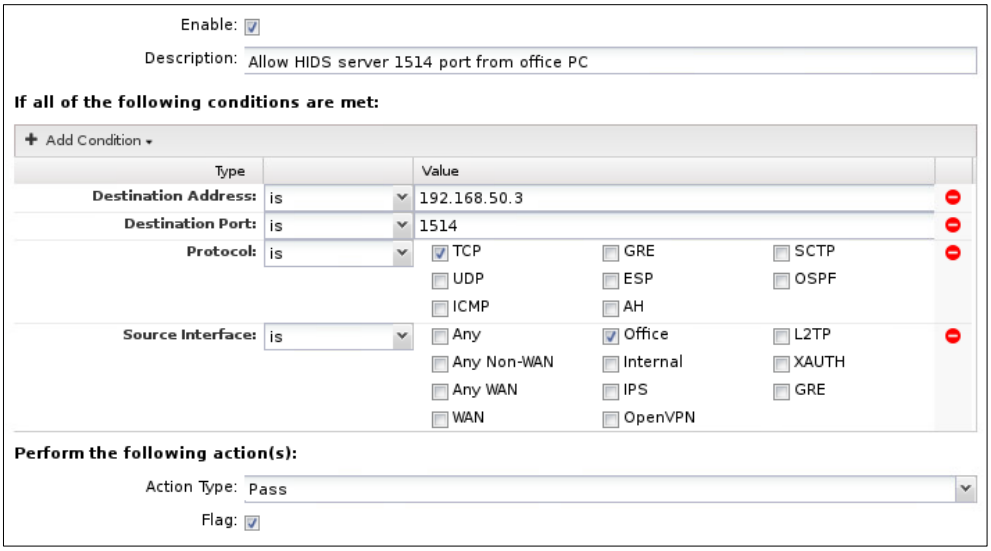


그림 3-16 Allow HIDS server 1514 port from office PC

Office망에 있는 PC에서 HIDS 관리 서버(192.168.50.3) 접근이 가능하도록 그림 3-16과 같이 방화벽 룰을 설정한다. 룰의 id는 100004이다.

```
[root@localhost bin]# /var/ossec/bin/manage_agents -e 002

Agent key information for '002' is:
MDAyIGFnZW50X2RldmVsb3BlciAxOTIuMTY4LjQwLjIwMCAzMzI2ZDRlNDM5MmExNDNkZjRhMzMwZjJk
ZjU3NzJkYzEyZWMxMGZjMTBlY2YwODkyNjE4OWM0Y2I3ZmNhMWRi
```

그림 3-17 키 확인

관리 서버에서 `/var/ossec/bin/manage_agents -e [ID]` 명령어를 이용하여 각 에이전트에 할당된 키를 확인한다.

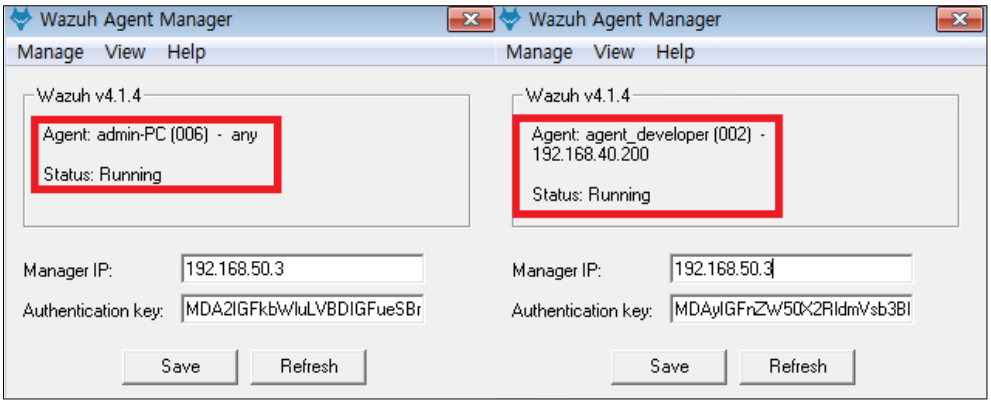


그림 3-18 에이전트 설정

Wazuh Agent Manager를 이용하여 각각의 에이전트 키 값을 설정한 후 실행한다.

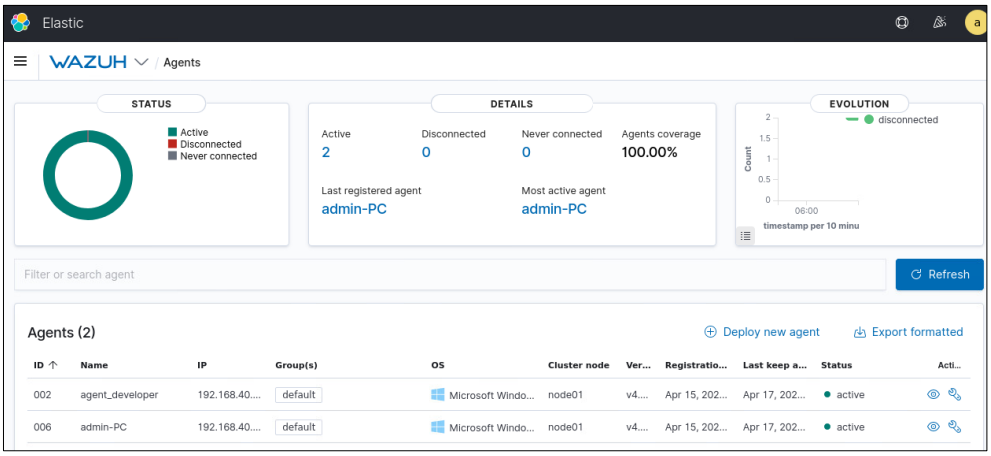


그림 3-19 active

Wazuh 관리 서버에서 확인한 결과 개발자PC, 관리자PC가 정상적으로 활성화되었다.

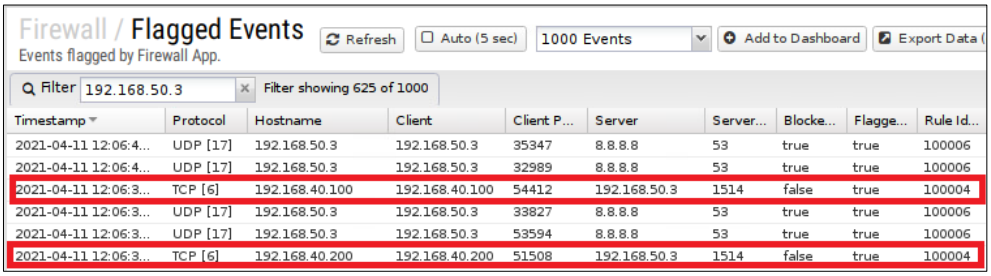


그림 3-20 Flagged Events

관리자PC(192.168.40.100)와 개발자PC(192.168.40.200)에서 HIDS 서버(192.168.50.3)로 접속할 때 방화벽 100004 룰에 의해 통과되었다.

3.5 관리자PC에서 HIDS 관리 서버 SSH 접속

HIDS 관리 서버는 Office망의 관리자PC만 SSH 포트 접속이 가능해야 한다.

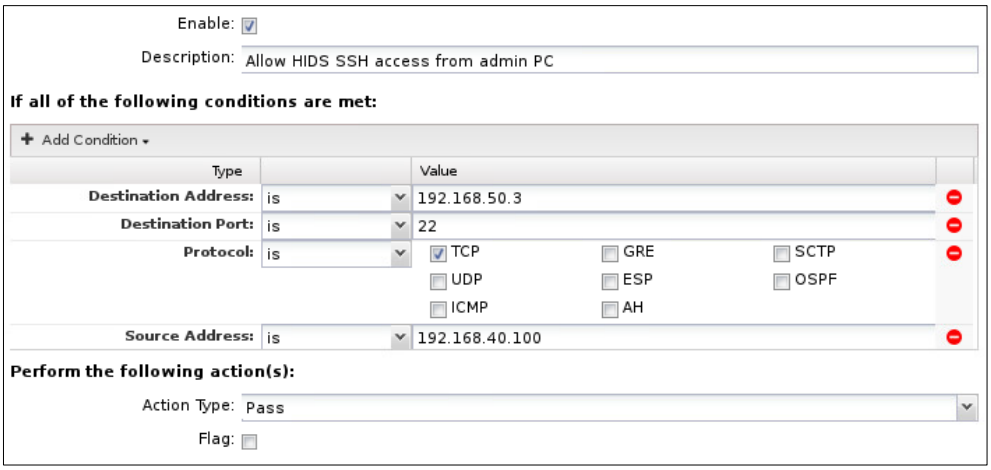


그림 3-21 Allow HIDS SSH access from admin PC

관리자PC(192.168.40.100)에서 HIDS 관리 서버(192.168.50.3) 접근이 가능하도록 그림 3-21과 같이 방화벽 룰을 설정한다. 룰의 id는 100005이다.

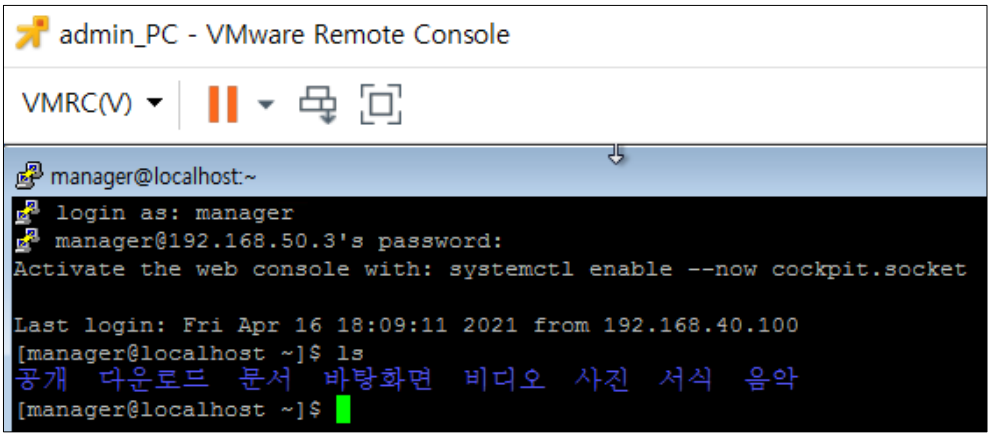


그림 3-22 SSH 접속 성공

관리자PC에서 SSH를 이용하여 HIDS 관리 서버 접근이 가능하다.

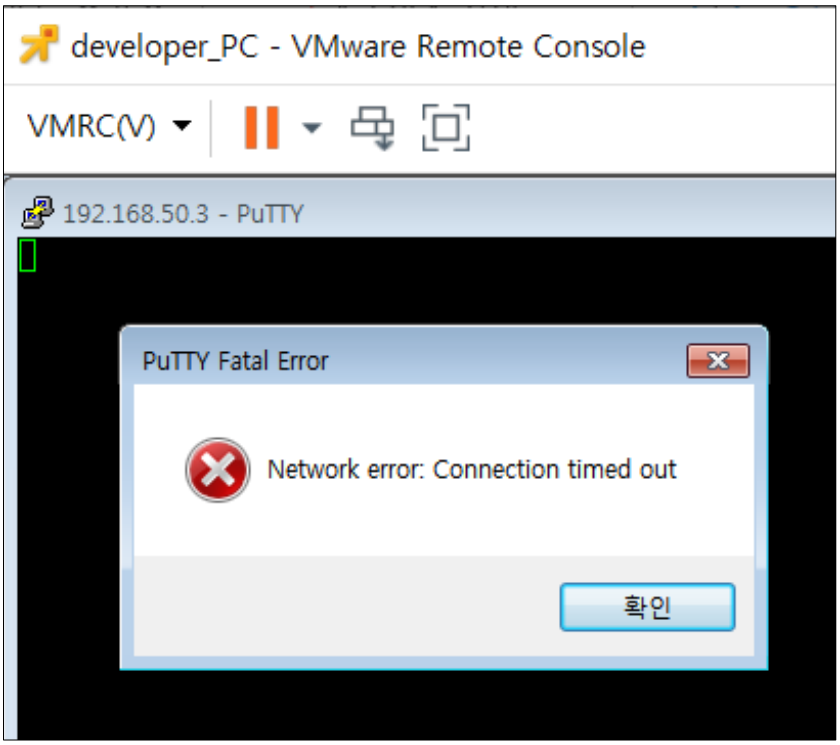


그림 3-23 SSH 접속 실패

개발자PC에서 SSH를 이용하여 HIDS 관리 서버 접근이 불가능하다.

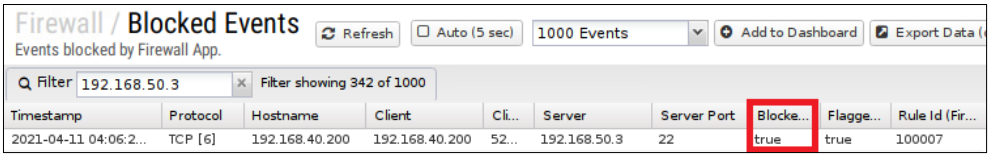


그림 3-24 Flagged Events

개발자PC(192.168.40.200)에서 HIDS 관리 서버(192.168.50.3)로 SSH 접속할 때 방화벽 100007 룰에 의해 거부되었다.

3.6 관리자PC에서 방화벽 관리 페이지 접속

방화벽 관리 페이지는 오직 관리자 PC에서만 접속이 가능해야 한다.

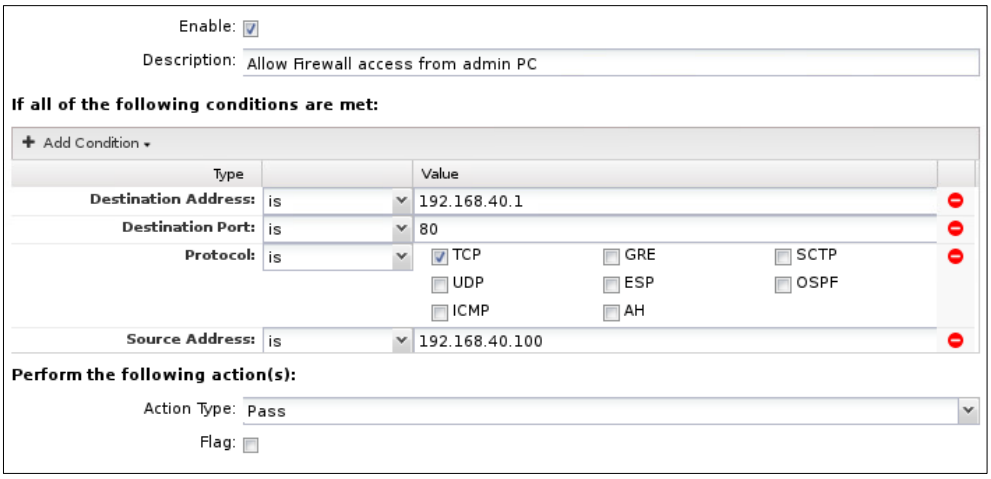


그림 3-25 Allow Firewall access from admin PC

관리자PC(192.168.40.100)에서만 방화벽 관리 페이지 접근이 가능하도록 그림 3-25와 같이 방화벽 룰을 설정한다. 룰의 id는 100006이다.

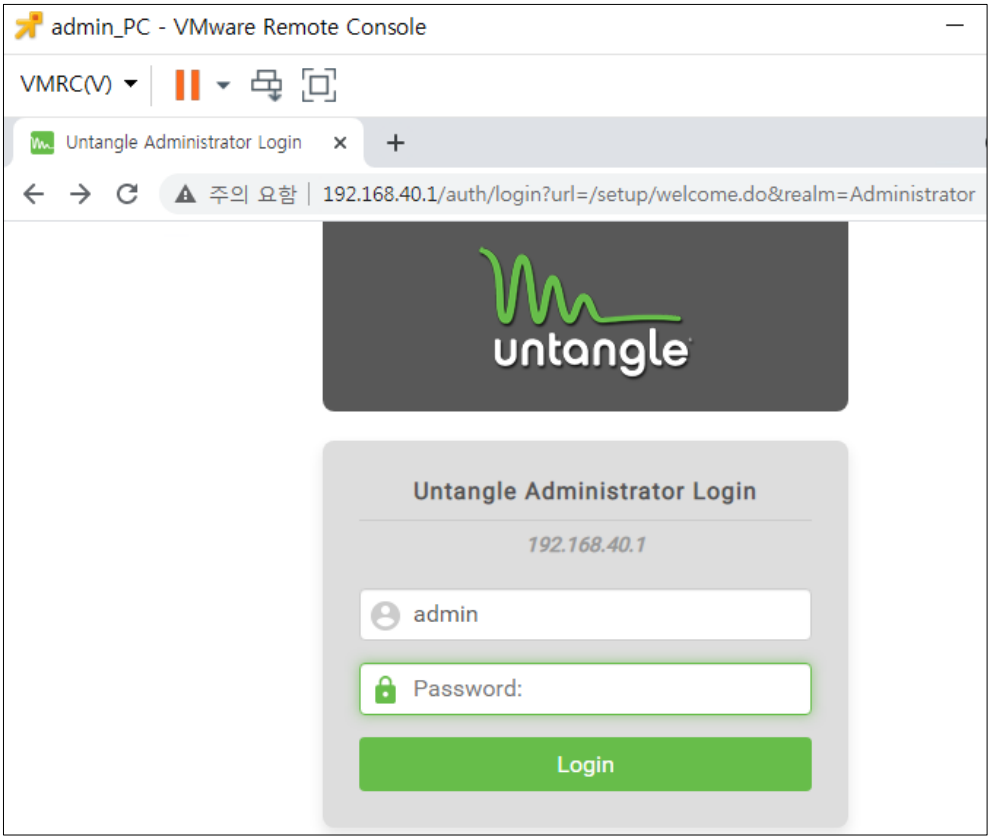


그림 3-26 관리자 페이지 접속 성공

관리자PC에서 방화벽 관리자 페이지 접근이 가능하다.

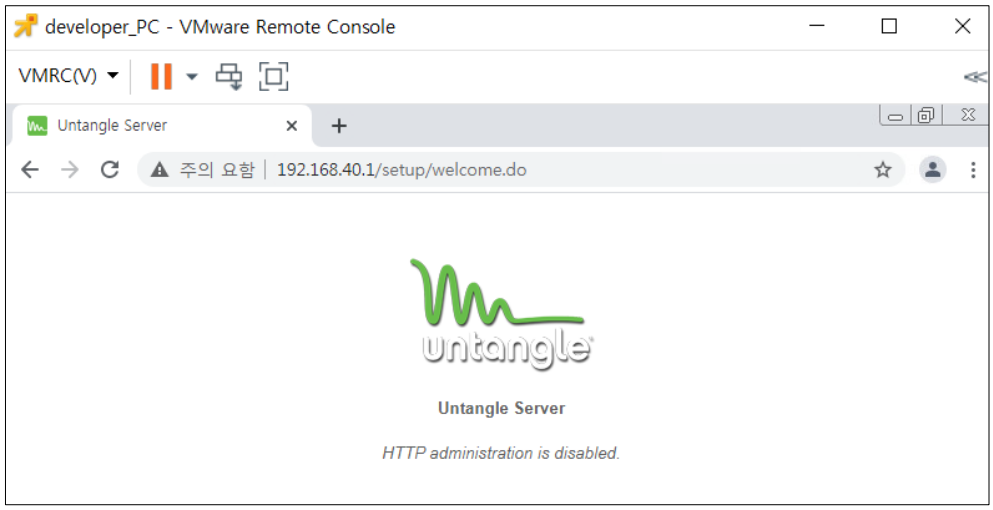


그림 3-27 관리자 페이지 접속 실패

관리자PC가 아닌 단말은 방화벽 관리자 페이지 접근이 불가능하다.

3.7 내부망에서 인터넷 접속

내부의 있는 모든 망은 외부와의 인터넷이 불가능해야 한다.

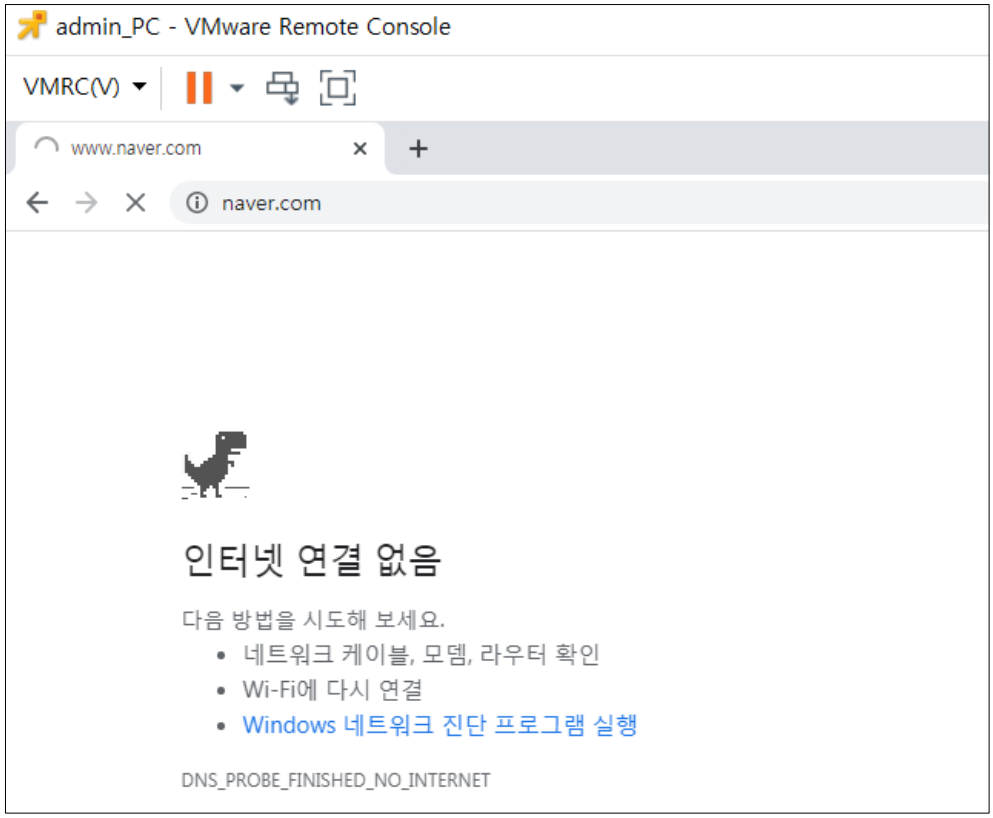


그림 3-28 인터넷 접속 불가

관리자PC에서 외부 인터넷 접속이 불가능하다.

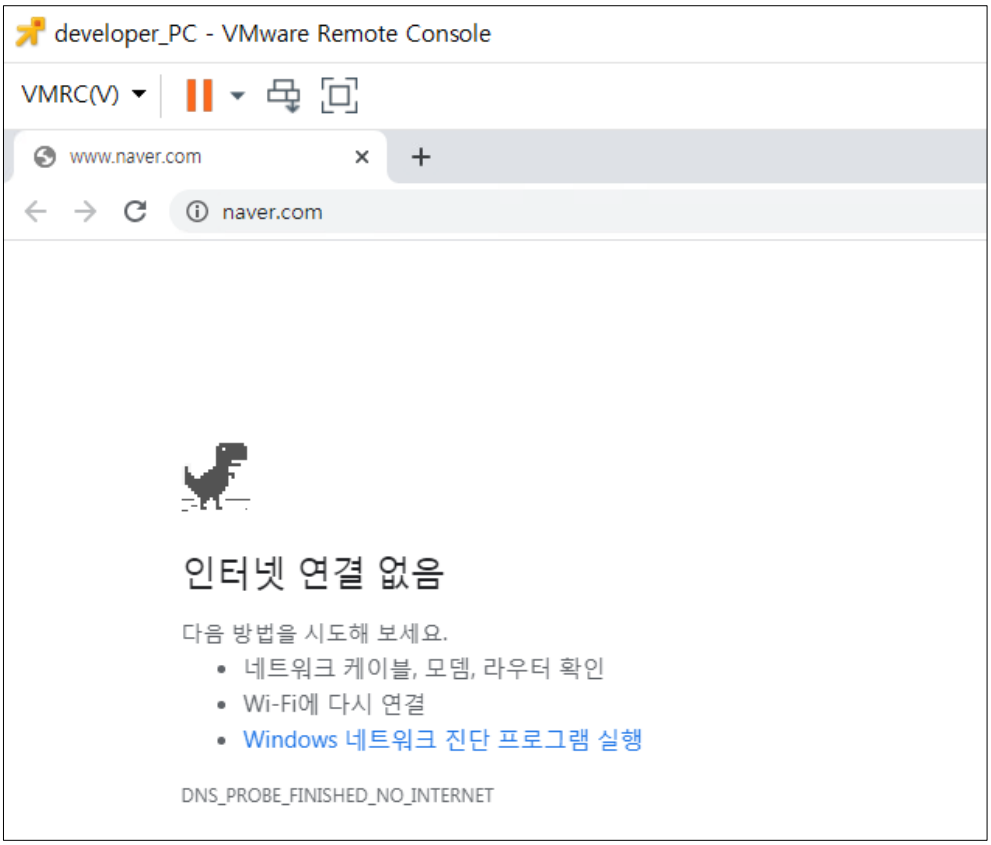


그림 3-29 인터넷 접속 불가

개발자PC에서 외부 인터넷 접속이 불가능하다.

3.8 방화벽 룰

	Rule Id	Enable	Description	Conditions	Block	Flag
✣	100001	☑	Allow WebServer access from wlan	Destination Address ⇒ 192.168.70.22 • Destination Port ⇒ 80 • Protocol ⇒ T...	☐	☑
✣	100002	☑	Allow WebServer HTTP access from dev...	Destination Address ⇒ 192.168.70.22 • Destination Port ⇒ 80 • Protocol ⇒ T...	☐	☑
✣	100003	☑	Allow WebServer SSH access from deve...	Destination Address ⇒ 192.168.70.22 • Destination Port ⇒ 22 • Protocol ⇒ T...	☐	☑
✣	100004	☑	Allow HIDS server 1514 port from office...	Destination Address ⇒ 192.168.50.3 • Destination Port ⇒ 1514 • Protocol ⇒ ...	☐	☑
✣	100005	☑	Allow HIDS SSH access from admin PC	Destination Address ⇒ 192.168.50.3 • Destination Port ⇒ 22 • Protocol ⇒ TC...	☐	☑
✣	100006	☑	Allow Firewall access from admin PC	Destination Address ⇒ 192.168.40.1 • Destination Port ⇒ 80 • Protocol ⇒ TC...	☐	☑
✣	100007	☑	Block All	*No conditions*	☑	☑

그림 3-30 방화벽 룰 목록

최종적으로 방화벽에 적용한 룰은 7개로 상세 목록은 그림 3-30과 같다.

4 참고 문헌

4.1 단행본

도서명	저자	출판사

표 4-1 단행본

4.2 참조 홈페이지

참조 홈페이지
https://forums.untangle.com/
https://psychoria.tistory.com/697
https://documentation.wazuh.com/current/installation-guide/open-distro/all-in-one-deployment/all_in_one.html
https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh_agent_package_windows.html#wazuh-agent-package-windows
https://library.gabia.com/contents/infrahosting/3472/

표 4-2 참조 홈페이지