네트워크 보안 평가 과제

DevSecOps 활용 클라우드 보안 전문가

작성자: 정재호

작성일: 2024.09.19

내용

[0. 평가 과제 4](#_Toc177660722)

[0.1. 평가 요소 4](#_Toc177660723)

[0.2. 평가 과제 4](#_Toc177660724)

[1. 네트워크 토폴로지 5](#_Toc177660725)

[1.1. IP 및 라우팅 프로토콜 설정 5](#_Toc177660726)

[1.2. ASAv-FW 인터페이스 zone 설정 6](#_Toc177660727)

[2. ASAv ACL 6](#_Toc177660728)

[2.1. ACL 요청 사항 6](#_Toc177660729)

[2.2. ASAv SSL Setting 6](#_Toc177660730)

[2.3. ASAv 접속 제어 7](#_Toc177660731)

[2.4. ACL 구문 7](#_Toc177660732)

[2.5. ACL 적용 결과 7](#_Toc177660733)

[3. Snort Rule 9](#_Toc177660734)

[3.1. Rule 요청 사항 9](#_Toc177660735)

[3.2. Custom Rules 9](#_Toc177660736)

[3.3. Snort Version Upgrade 10](#_Toc177660737)

[4. Zabbix Server 11](#_Toc177660738)

[4.1. 토폴로지 변경 사항 11](#_Toc177660739)

[4.2. Zabbix Agent 12](#_Toc177660740)

[5. pfsense 13](#_Toc177660741)

[5.1. 토폴로지 변경사항 13](#_Toc177660742)

[5.2. pfsense 설정 13](#_Toc177660743)

[5.3. Open VPN (진행 불가) 14](#_Toc177660744)

[6. Suricata Server 15](#_Toc177660745)

[6.1. 토폴로지 변경 사항 15](#_Toc177660746)

[Suricata Version Upgrade 16](#_Toc177660747)

[7. Attacker (Kali) 16](#_Toc177660748)

[7.1. 공격 탐지 16](#_Toc177660749)

[7.2. 최신 네트워크 보안 솔루션 동향 조사 16](#_Toc177660750)

# 0. 평가 과제

## 0.1. 평가 요소

- 네트워크 보안 설계, 네트워크 보안 구현

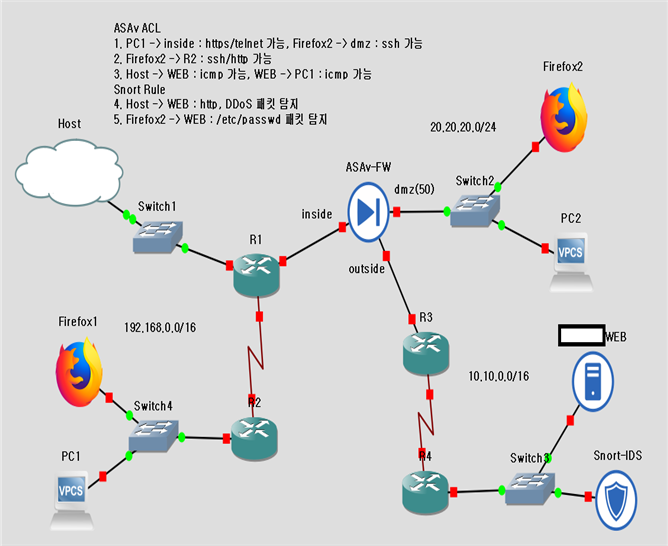
- 네트워크 보안 솔루션 운영, 네트워크 보안 솔루션 운영 개선

- 네트워크 보안 신규 위협 대응, 네트워크 보안 솔루션 업데이트 적용

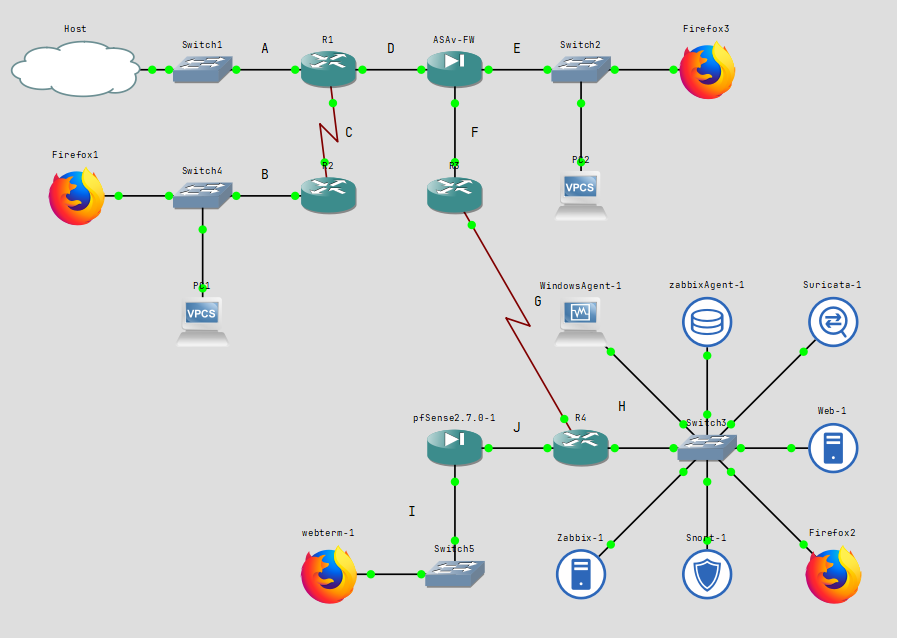
## 0.2. 평가 과제

“Koreait 사이트에서 기존의 방화벽 외 IDS(NIDS, HIDS)장비를 추가하여 네트워크 트래픽을 탐지 운영을 시작하게 되었다. 이 때 이벤트 분석 및 탐지를 위한 여러 도구를 활용하고 Snort Rule을 통해 해당 문제를 해결하고 pfsense 솔루션을 통해 OpenVPN(remote access VPN)을 설정하여 접속할 수 있도록 설정해라

GNS3 프로그램을 통해 제공된 토폴로지를 설정하고 Firewall(ASAv-방화벽) 및 IDS(Snort-침입탐지시스템)를 정책 요청에 맞게 설정해라”



# 1. 네트워크 토폴로지



## 1.1. IP 및 라우팅 프로토콜 설정

|  |  |  |
| --- | --- | --- |
| **네트워크 명칭** | **네트워크 대역** | **IP 할당 내역** |
| A\_Network | 192.168.0.0/18 | Host: 192.168.0.1  R1(f0/0), Gateway: 192.168.63.254 |
| B\_Network | 192.168.64.0/18 | Firefox1: 192.168.64.1  PC1: 192.168.64.2  R2(f0/0), Gateway: 192.168.127.254 |
| C\_Network | 192.168.128.0/18 | R1(s0/0): 192.168.128.1  R2(s0/0): 192.168.128.2 |
| D\_Network | 20.20.20.0/26 | R1(f0/1): 20.20.20.1  ASAv-FW(gi0/1): 20.20.20.2 |
| E\_Network | 20.20.20.64/26 | ASAv-FW(gi0/0), Gateway: 20.20.20.126  Firefox2: 20.20.20.65  PC2: 20.20.20.66 |
| F\_Network | 20.20.20.128/26 | ASAv-FW(gi0/2): 20.20.20.129  R3(f0/0): 20.20.20.130 |
| G\_Network | 10.10.0.0/17 | R3(s0/0): 10.10.0.1  R4(s0/0): 10.10.0.2 |
| H\_Network | 10.10.128.0/17 | R4(f0/0), Gateway: 10.10.255.254  WEB: 10.10.128.1  Snort-IDS: 10.10.128.2 |
| I\_Network | 1.1.1.0/24 | Pfsense(Lan): 1.1.1.254  Webterm-1: 1.1.1.1 |
| J\_Network | 2.2.2.0/24 | Pfsense(Wan): 2.2.2.1  R4(f0/1): 2.2.2.2 |

- 모두 OSPF 라우팅 프로토콜을 채택

## 1.2. ASAv-FW 인터페이스 zone 설정

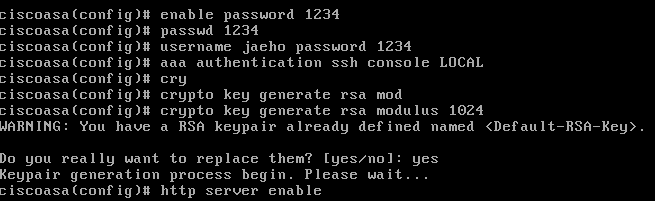
|  |  |  |  |
| --- | --- | --- | --- |
|  | **인터페이스** | **존 명칭** | **보안 레벨** |
| Gi0/0 | outside | 0 |
| Gi0/1 | inside | 100 |
| Gi0/2 | dmz | 50 |

# 2. ASAv ACL

## 2.1. ACL 요청 사항

|  |  |  |
| --- | --- | --- |
| **번호** | **대상** | **내용** |
| 1 | PC1 > inside | * https/telnet 허용 |
| 2 | Firefox2 > dmz | * ssh 허용 |
| 3 | Firefox2 > R2 | * ssh/http 허용 |
| 4 | Host > WEB | * icmp 허용 |
| 5 | WEB > PC1 | * icmp 허용 |

## 2.2. ASAv SSL Setting



## 2.3. ASAv 접속 제어

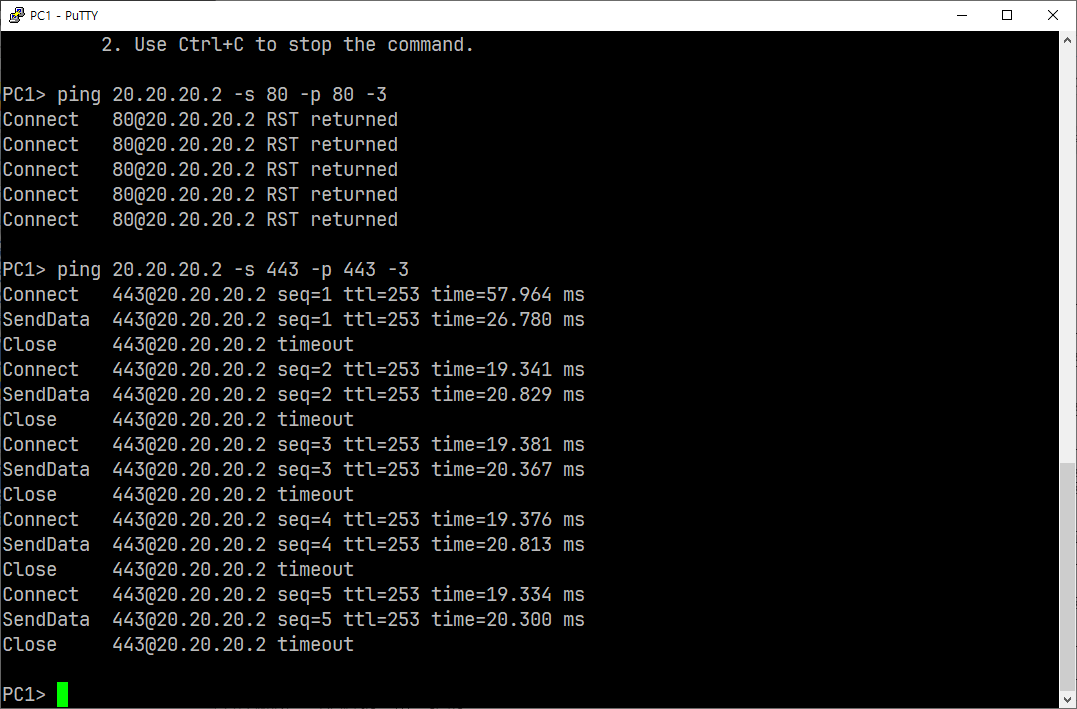
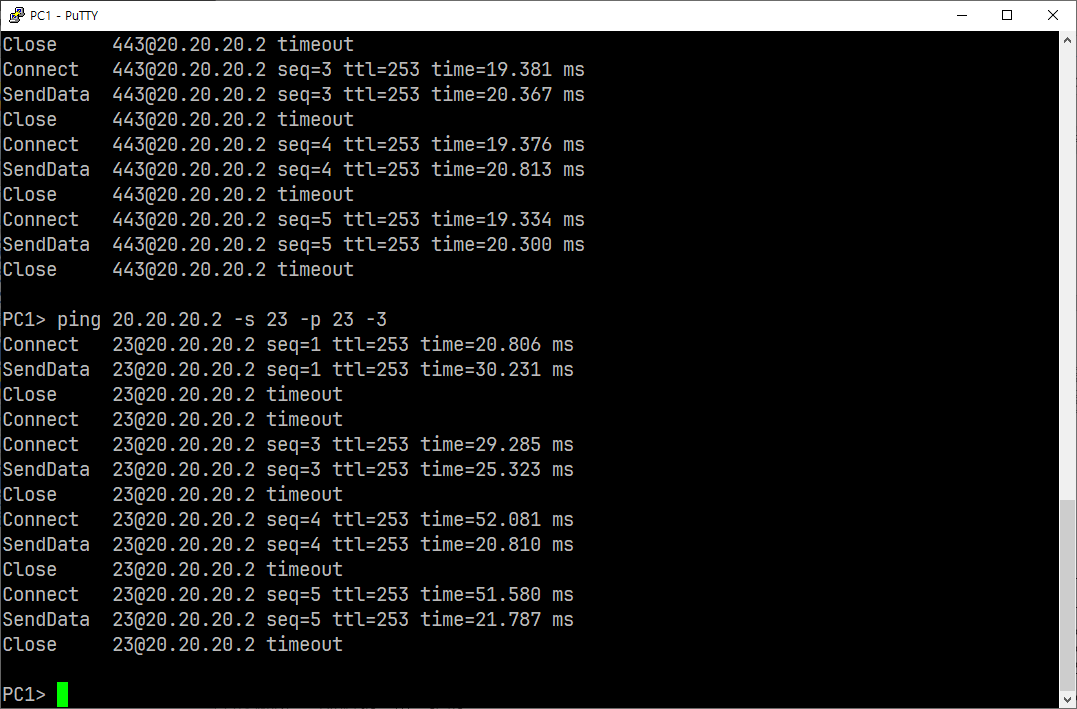


## 2.4. ACL 구문

|  |  |
| --- | --- |
| **zone** | **ACL 정책** |
| dmz | access-group dmzin in interface dmz  access-list dmzin extended permit tcp host 20.20.20.65 host 20.20.20.126 eq ssh  access-list dmzin extended permit tcp host 20.20.20.65 host 192.168.128.2 eq ssh  access-list dmzin extended permit tcp host 20.20.20.65 host 192.168.128.2 eq www |
| inside | access-group inout in interface inside  access-list inout extended permit tcp host 192.168.64.2 host 20.20.20.2 eq www  access-list inout extended permit tcp host 192.168.64.2 host 20.20.20.2 eq telnet  access-list inout extended permit icmp host 192.168.0.1 host 10.10.128.1 echo  access-list inout extended permit icmp host 192.168.0.1 host 10.10.128.1 echo-reply  access-list inout extended permit icmp host 192.168.64.2 host 10.10.128.1 echo-reply |
| outside | access-group outin in interface outside  access-list outin extended permit icmp host 10.10.128.1 host 192.168.0.1 echo-reply  access-list outin extended permit icmp host 10.10.128.1 host 192.168.64.2 echo  access-list outin extended permit icmp host 10.10.128.1 host 192.168.64.2 echo-reply |

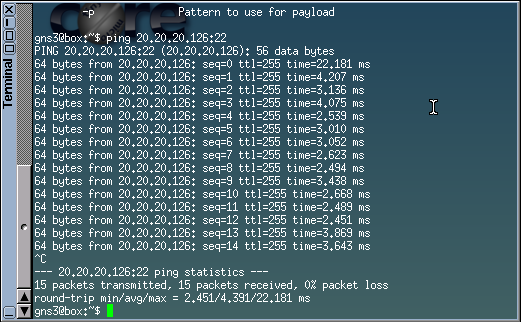
## 2.5. ACL 적용 결과

### 1) PC1 > inside

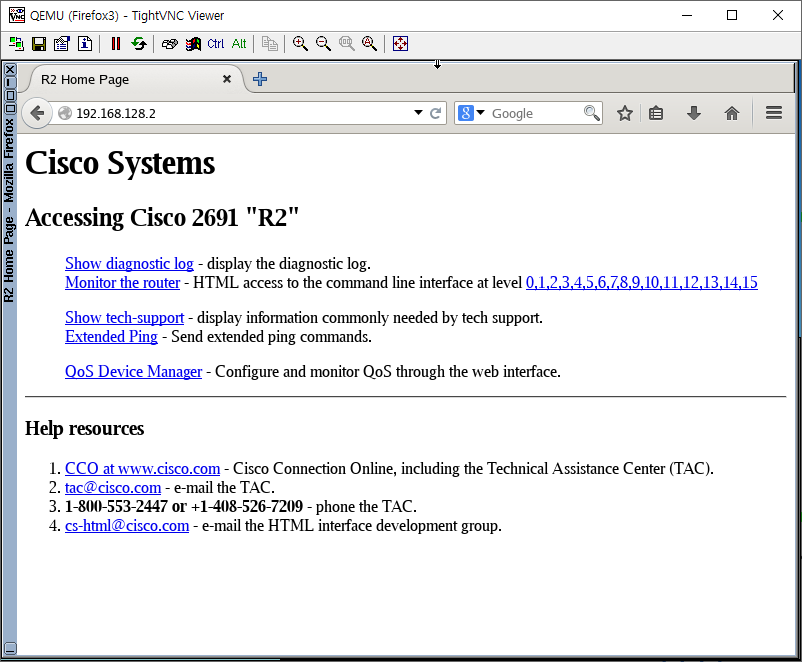
 

- 좌) http/https 테스트 , 우) telnet 테스트

### 2) Firefox2 > dmz



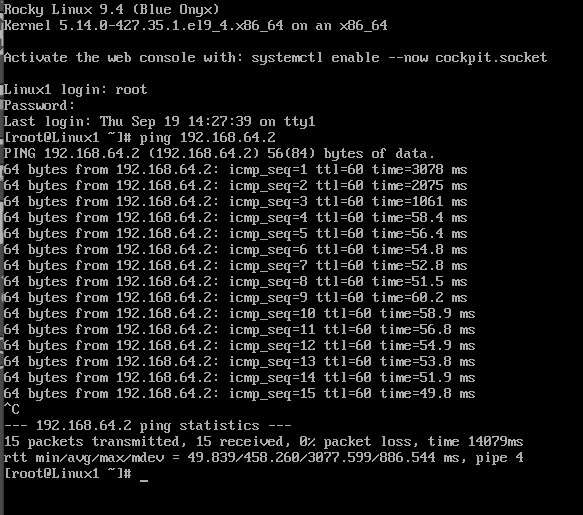
### 3) Firefox2 > R2



### 4) Host > WEB

- 해당 장치는 연결할 수 없는 상태로 인해 테스트 불가능

### 5) WEB > PC1



# 3. Snort Rule

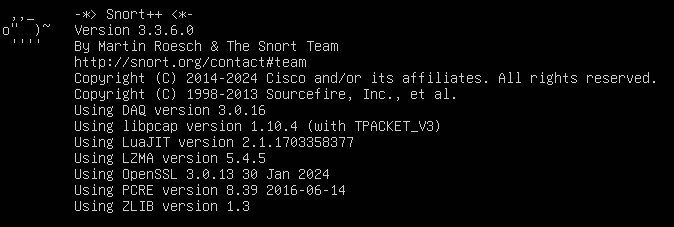
## 3.1. Rule 요청 사항

|  |  |  |
| --- | --- | --- |
| **번호** | **대상** | **내용** |
| 1 | Host > WEB | * http, DDoS 패킷 탐지 |
| 2 | Firefox2 > WEB | * /etc/passwd 패킷 탐지 |

## 3.2. Custom Rules

|  |
| --- |
| # 1 Host > WEB - http, DDoS 패킷 탐지  alert tcp 192.168.0.1 any -> 10.10.128.1 80 (msg:"tcp http alert";sid:1000001;rev:1;)  alert icmp 192.168.0.1 any -> 10.10.128.1 any (msg:"DDoS Attack alert";sid:1000002;rev:1;) |
| Host 네트워크에서 WEB 서버로 http 접속(DDoS 공격)을 시도할 환경 세팅에 문제가 있어 테스트는 추후로 미룸 |
| # 2 Firefox2 > WEB - /etc/passwd 패킷 탐지 (Encoding 감지)  alert tcp 20.20.20.65 any -> 10.10.128.1 80 (msg:"Attempt to access /etc/passwd"; content:"/etc/passwd"; http\_uri; sid:1000003; rev:2;)  alert tcp any any -> 10.10.128.1 80 (msg:"Encoded attempt to access /etc/passwd"; content:"%2Fetc%2Fpasswd"; http\_uri; sid:1000004; rev:1;) |
|  |
|  |

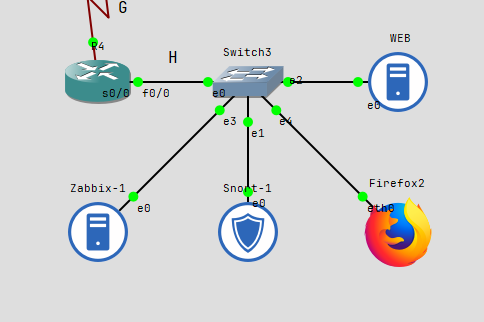
## 3.3. Snort Version Upgrade



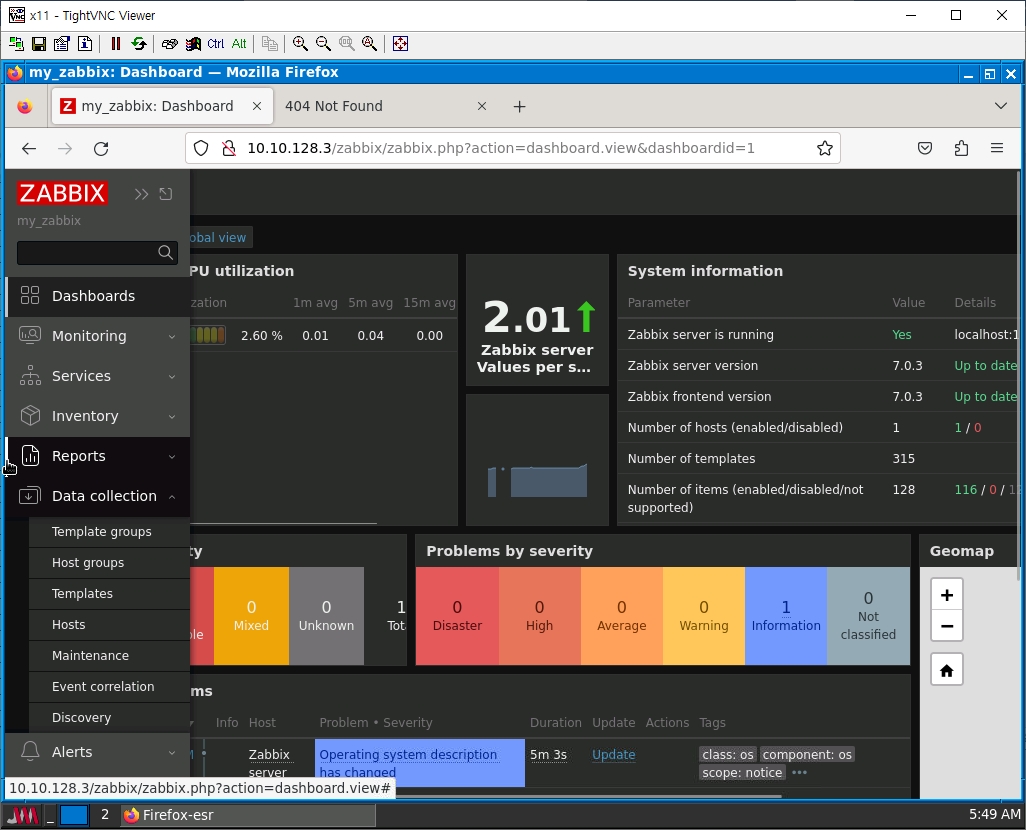
* 현재 Snort 버전 최신 버전으로 확인된다.

# 4. Zabbix Server

## 4.1. 토폴로지 변경 사항

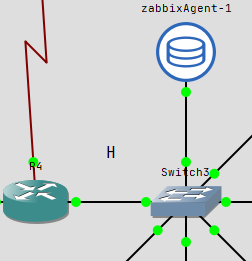
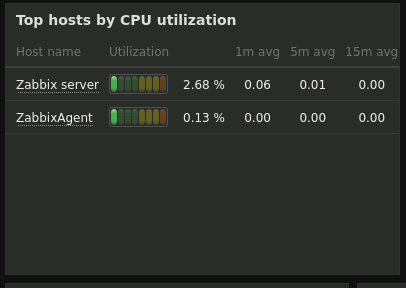


* Zabbix Server 장치를 H 네트워크에 추가 설치했다.
* 아래는 Firefox2 장치를 통해 웹 접속을 시도한 결과이다.



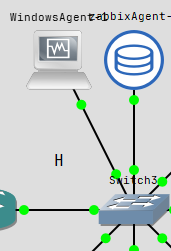
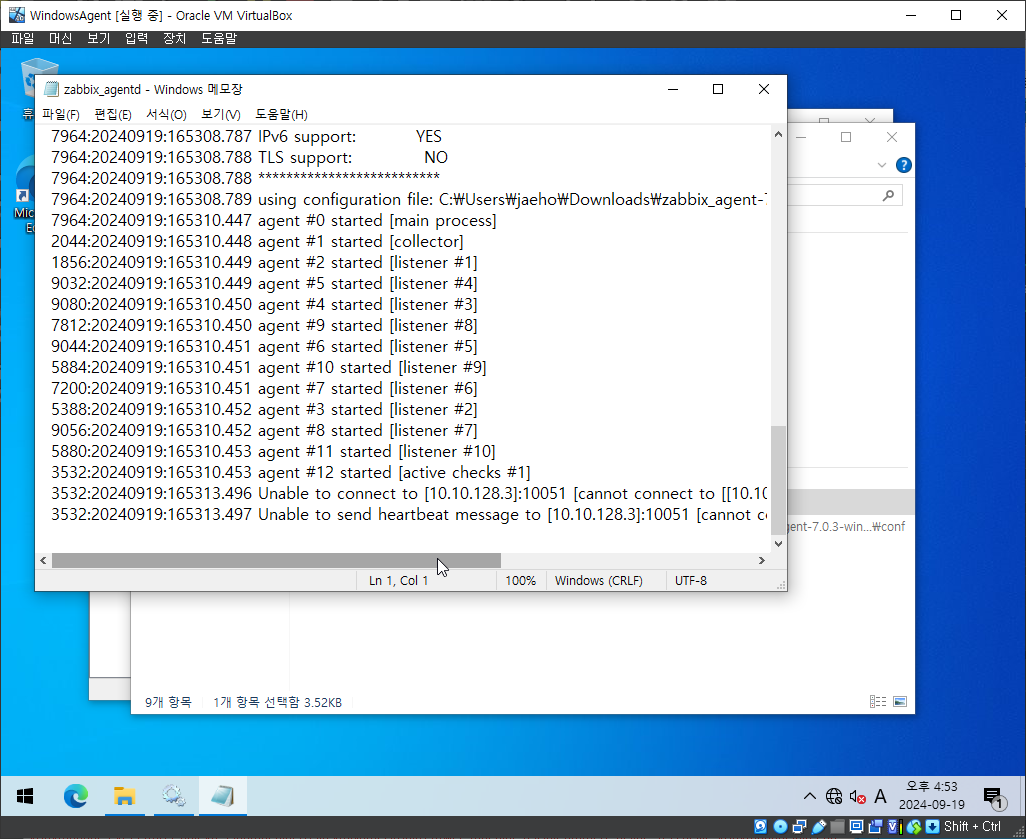
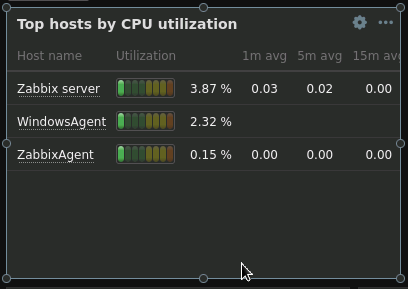
## 4.2. Zabbix Agent

### 1) Linux Zabbix Agent

- H 네트워크에 10.10.128.20 IP를 할당하여 Agent를 추가했다.

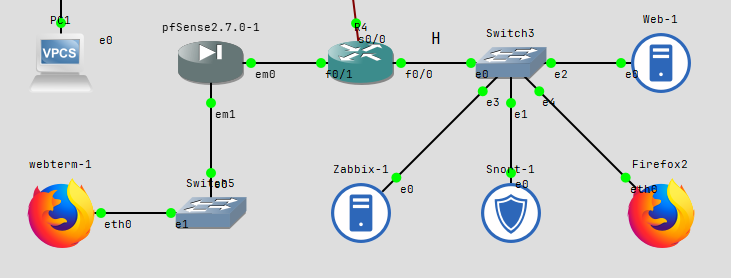
### 2) Windows Zabbix Agent

- H 네트워크에 10.10.128.25 IP 의 Windows Agent를 추가했다.

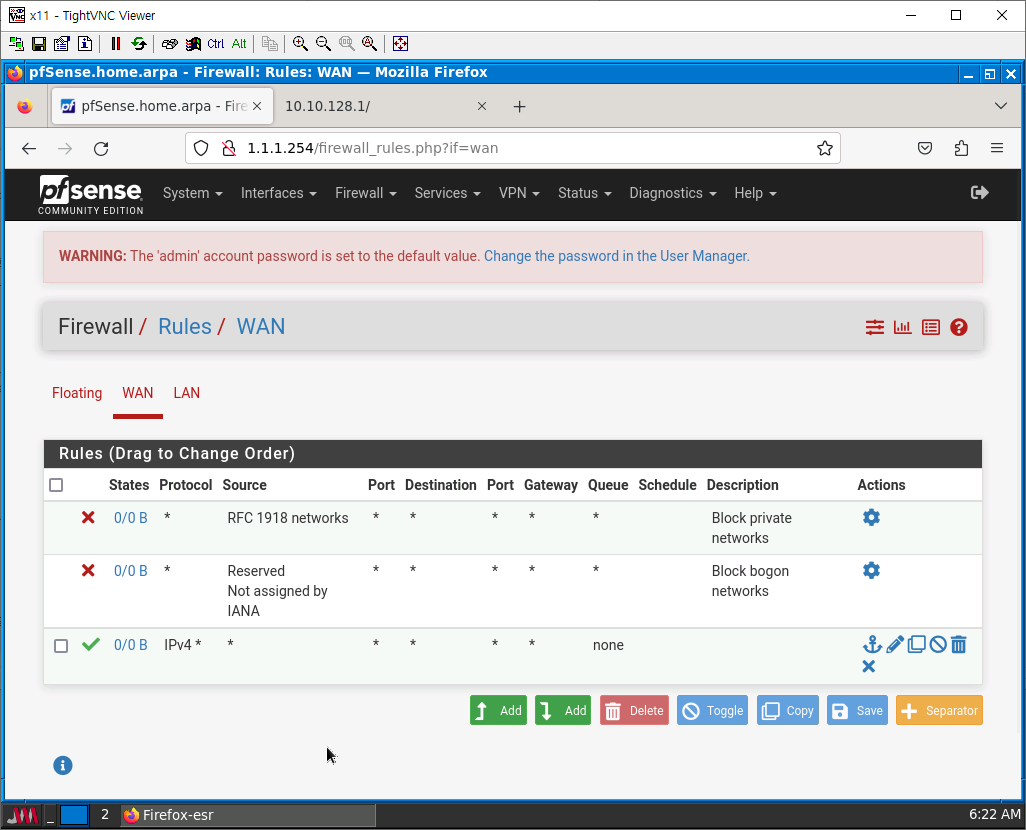
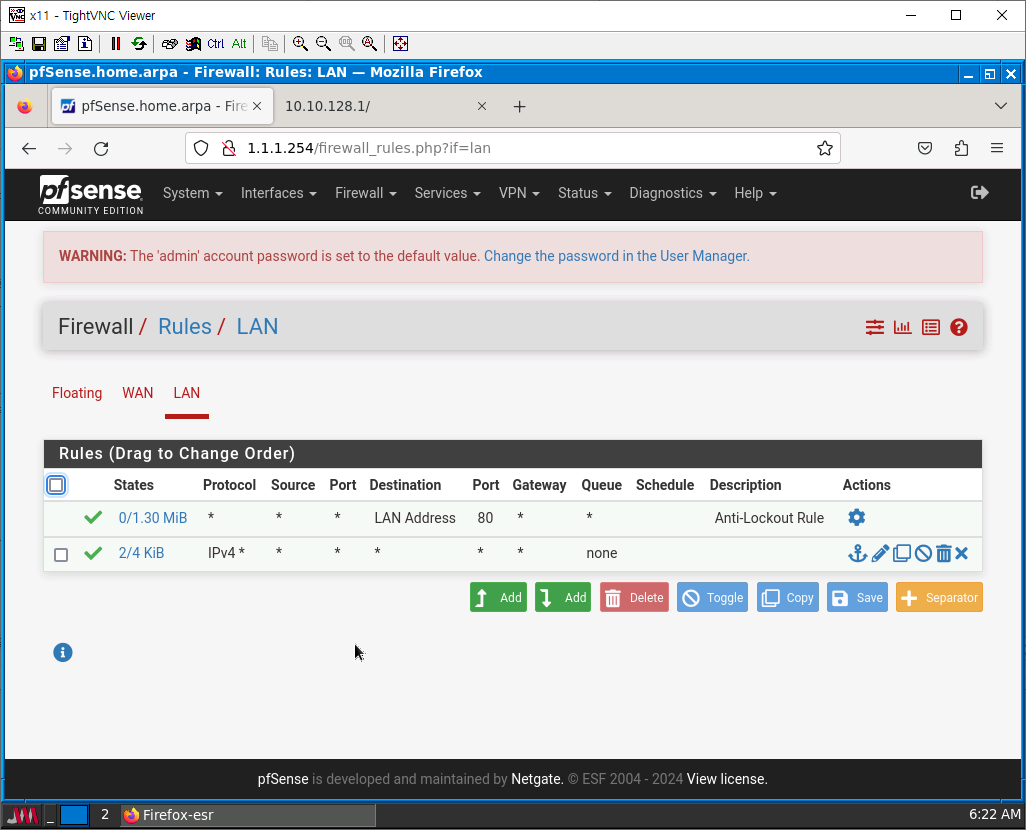
# 5. pfsense

## 5.1. 토폴로지 변경사항



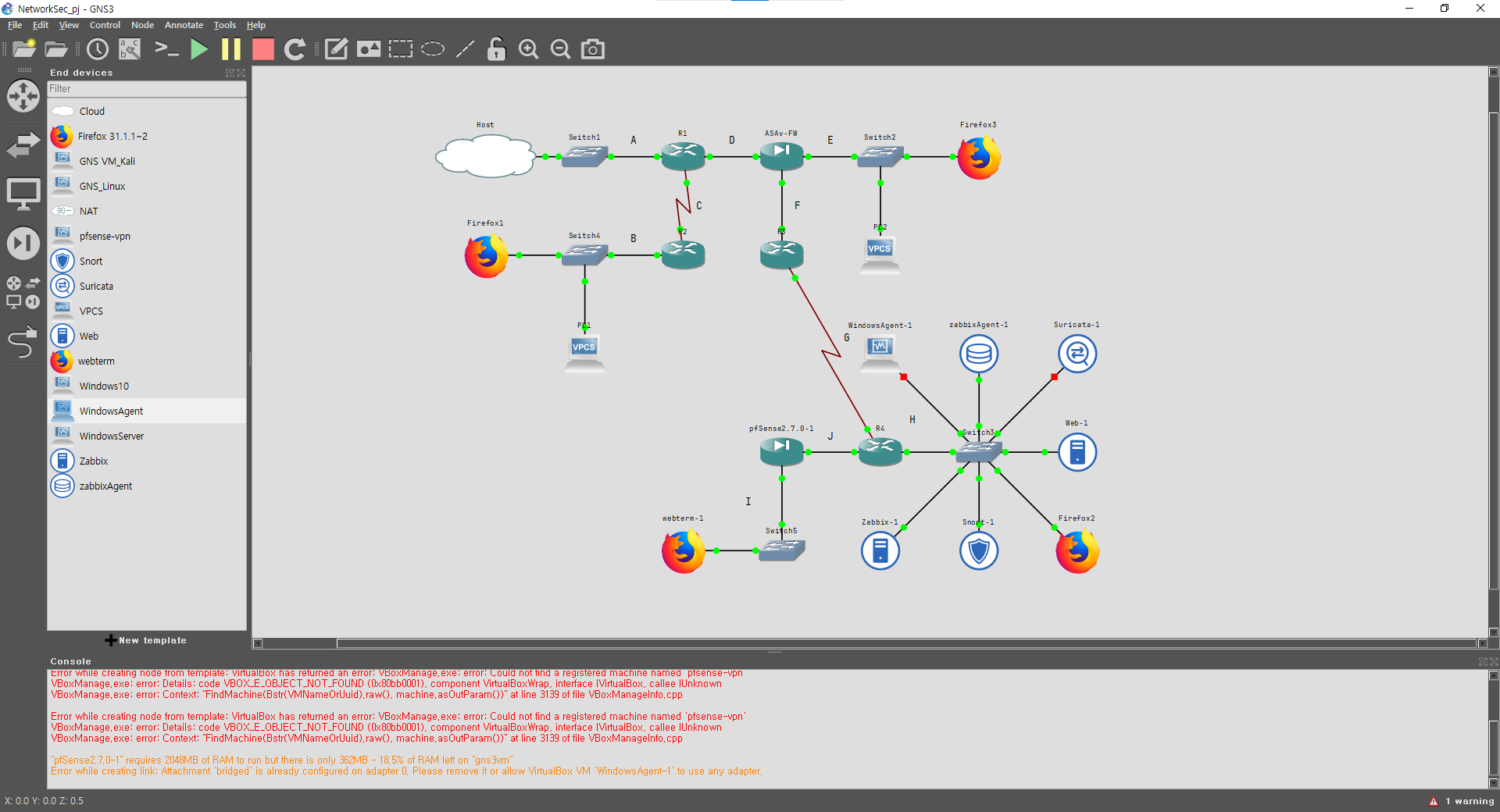
* R4 라우터와 새로 연결된 pfsense 장치 추가

## 5.2. pfsense 설정

* R4와 Static 라우팅 후 방화벽 설정에서 모든 패킷을 허용

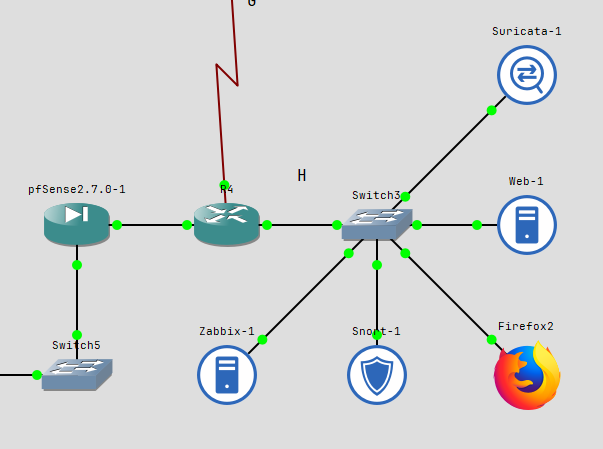
## 5.3. Open VPN (진행 불가)

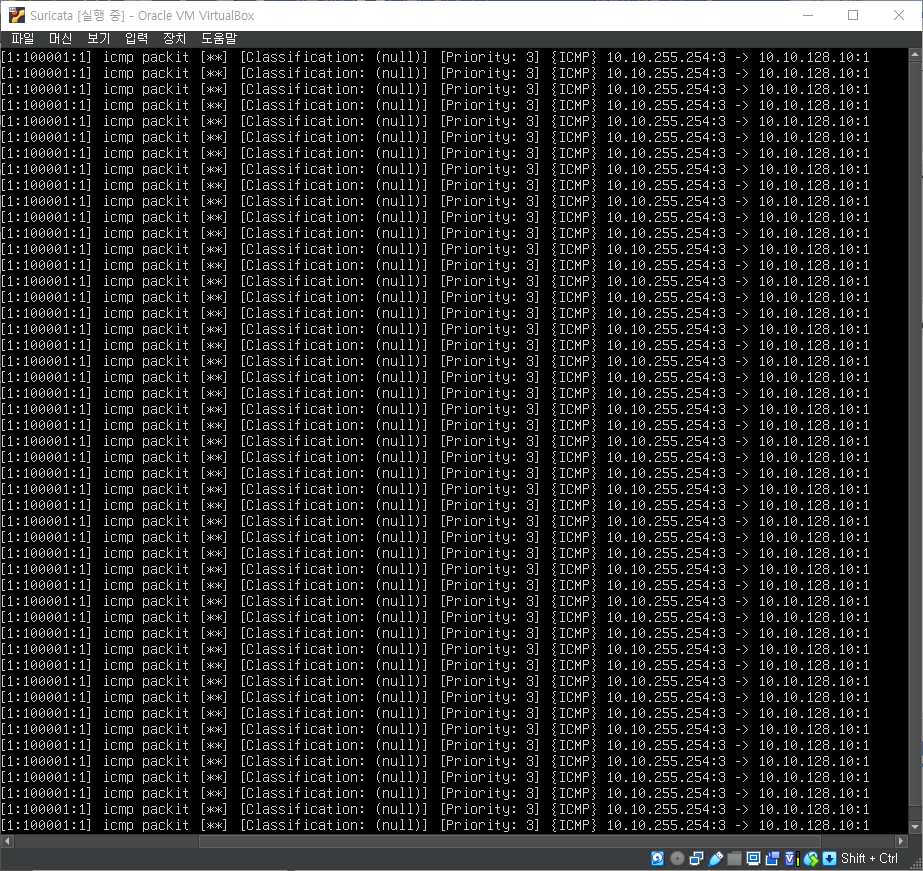


* 현재 작업 환경을 GNS3 프로젝트 파일 내 모두 구현하며 작업하는 바람에 pfsense 플러그인을 활용한 Open VPN을 사용할 수 없는 상황이 발생
* 과제 제출 전 시간이 남는다면 별도의 환경에서 작업 후 자료 첨부 예정

# 6. Suricata Server

## 6.1. 토폴로지 변경 사항



* 10.10.128.0/17 네트워크에 Suricata Server 장치를 추가 설치
* 10.10.128.10 IP 부여
* 테스트 목적으로 설정한 Rule로 인해 정상 작동 확인  
  alert icmp any any -> $HOME\_NET any (msg:"icmp packit";sid:100001;rev:1;)  
  

## Suricata Version Upgrade



- 최신 릴리즈 설치로 인해 버전 업그레이드가 필요 없어졌다.

# 7. Attacker (Kali)

## 7.1. 공격 탐지

**Attaker(kali)에서 Web Server로의 NIDS(Snort) 정책에 TCP Header에 SYN, flags를 탐지하는 룰과 DDoS 공격을 작성하는 Rule를 작성하여 탐지가 가능하도록 설정한 다음**

**Wireshark로 패킷을 캡처하여 내용을 확인하시오.**

* 시간 관계상 미 수행

## 7.2. 최신 네트워크 보안 솔루션 동향 조사

### 1) 제로 트러스트 아키텍처

- 기존 내부 망 또한 신뢰할 수 없다는 전제 조건하에 모든 접근에 대해 검증 절차를 진행하는 방식

- 최근 많아진 원격 업무(재택 근무)의 영향으로 낮아진 보안성을 올릴 수 있는 방안이라 많은 사람들이 생각하여 주목을 받고 있다고 한다.

### 2) IPS (Intrusion Prevention System)

- IDS의 확장 형태, 악의적인 행동을 탐지하고 차단하는 역할을 수행

- HTTP, FTP 등 TCP 또는 UDP 프로토콜을 검사, 네트워크 기반에서 위협을 탐지하고 차단

- NIPS, WIPS, HIPS 등으로 구분된다고 한다.  
(각각 네트워크, 무선, 호스트 기반에서 의심스러운 활동을 식별)

- IPS는 공격을 실시간으로 탐지하고 차단함으로 네트워크 안전성을 강화할 수 있다고 생각한다.