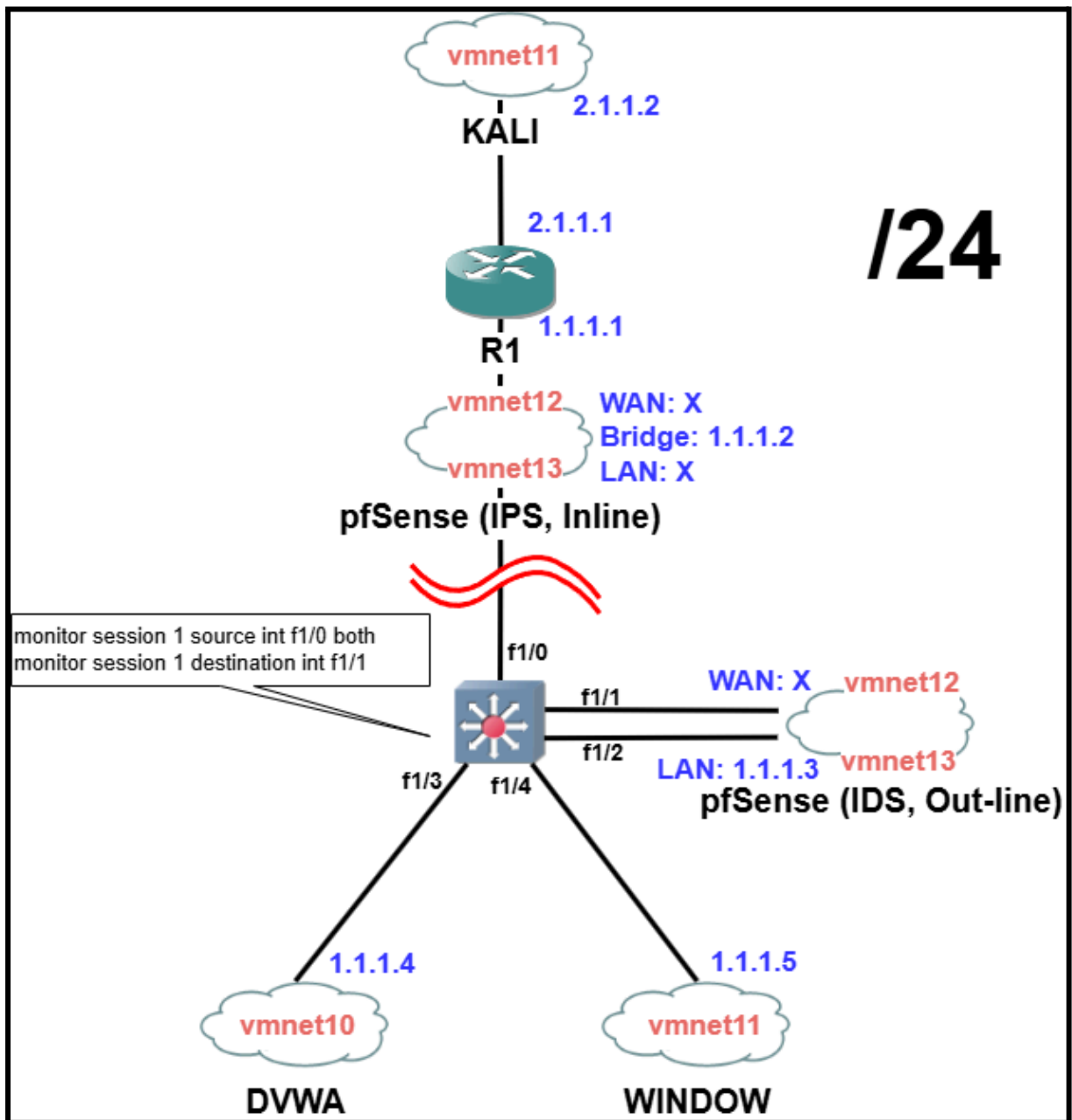


목차



1. 준비물

- pfSense
- (Kali linux) or (DVWA & Windows 10)
- GNS3

2. 실습용 사전 설치

- bridge망에서 pfsense 패키지 (snort, suricata) 설치
- windows에서 firefox 설치

3. pfSense에서 IPS, IDS 설정

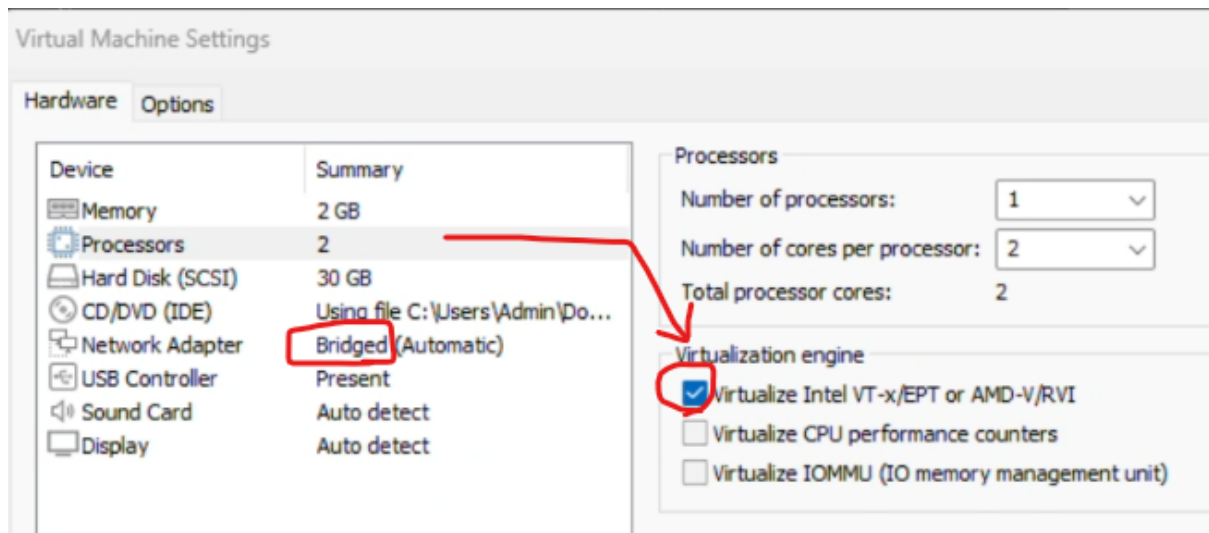
- 주의: 컨 채로 NIC 조작 금지, 설정 파일 함부로 수정하지 않기

4. 네트워크 토폴로지 적용

5. ruleset 테스트

- 간단한 ICMP 패킷 alert & drop 테스트
- Javascript attack 테스트
- nmap -v -sU -T4 -F 1.1.1.4 테스트

pfsense 초기 구성



Bridge에서 Snort, Suricata 패키지 설치 진행

- vm을 끈 상태에서 진행
- 편의상 Network Adapter 하나 삭제
- 프로세서에서 가상화 엔진 옵션 켜기

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 454db2b96e3a03541aa0
*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 172.16.129.131/16

0) Logout / Disconnect SSH
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset admin account and password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

9) pfTop
10) Filter Logs
11) Restart GUI
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

Enter an option: 4

You are about to reset the firewall to factory defaults.
The firewall will reboot after resetting the configuration.
All additional packages installed will be removed.
Do you want to proceed [y:n]? 
```

설정 동기화를 위한 공장초기화 (4번)

If the names of the interfaces are not known, auto-detection can be used instead. To use auto-detection, please disconnect all interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(a or nothing if finished):

WAN 인터페이스: em0

LAN 인터페이스: 미지정 (그냥 엔터)

```
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense 2.8.1-RELEASE amd64 20260701-1525
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 454db2b96e3a03541aa0

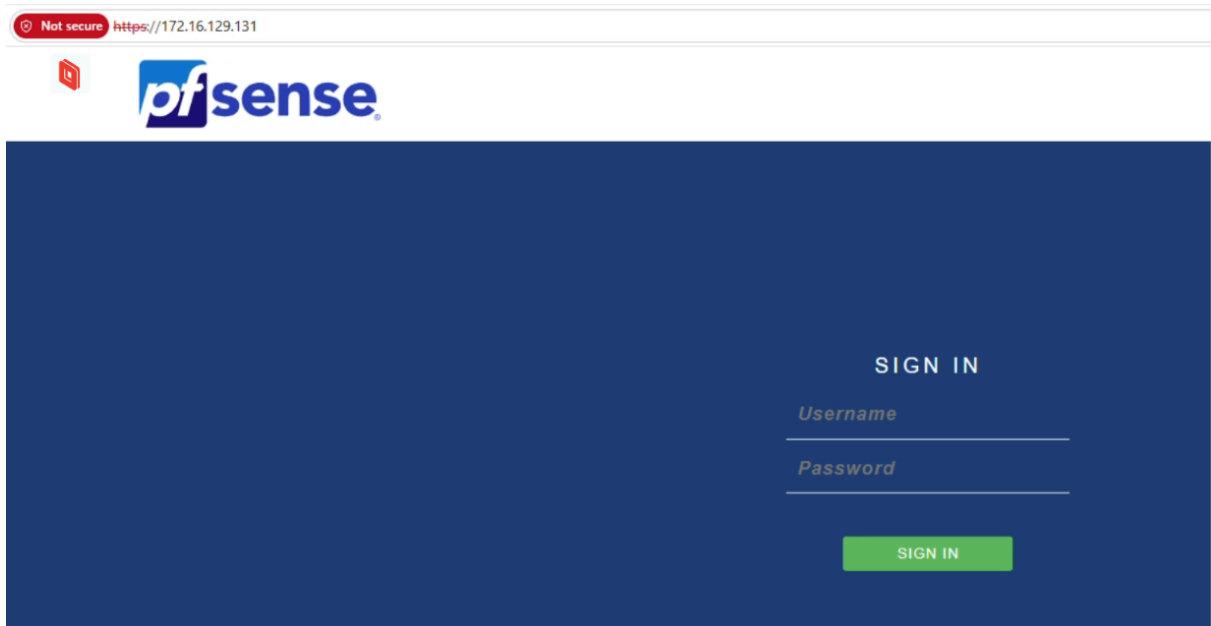
*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 172.16.129.131/16

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                    14) Enable Secure Shell (sshd)
6) Halt system                      15) Restore recent configuration
7) Ping host                        16) Restart PHP-FPM
8) Shell

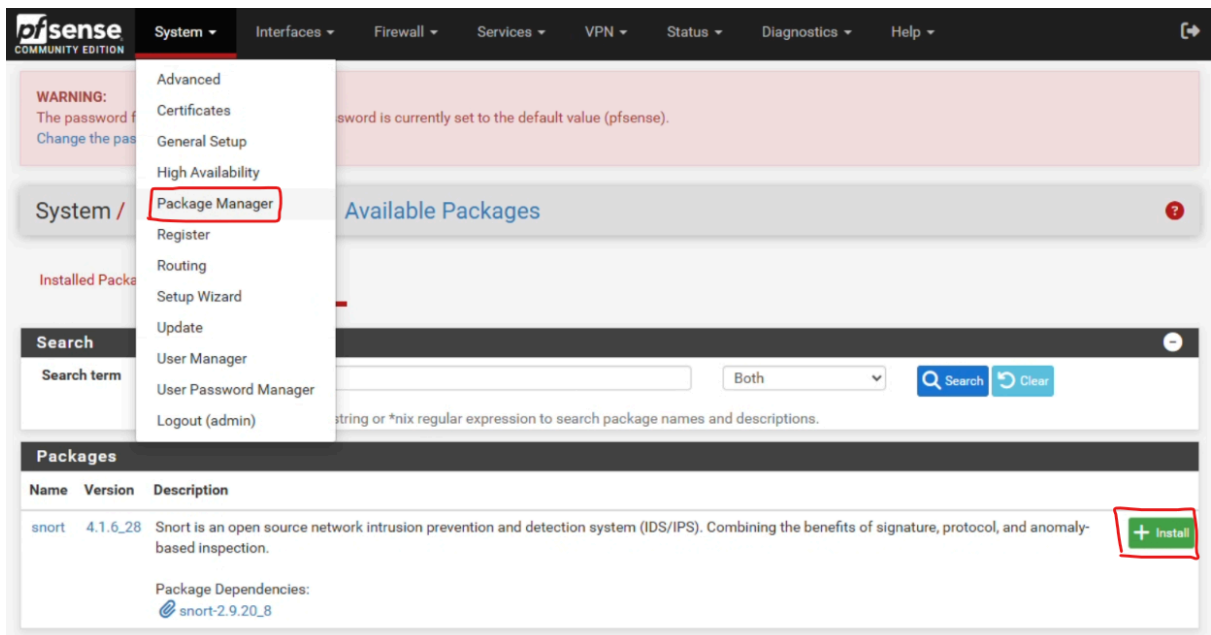
Enter an option:
```

DHCP를 통해 할당받은 IP로 웹 GUI 진입



초기 아이디: admin

초기 비밀번호: pfsense



Package Manager에서 snort, suricata 다운로드

```

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 454db2b96e3a03541aa0
*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 172.16.129.131/16

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address     11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                    14) Enable Secure Shell (sshd)
6) Halt system                      15) Restore recent configuration
7) Ping host                        16) Restart PHP-FPM
8) Shell

Enter an option: █

```

시스템 종료 (6번)

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	30 GB
CD/DVD (IDE)	Using file C:\Users\Admin\Do...
Network Adapter	Custom (VMnet12)
Network Adapter 2	Custom (VMnet13)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

NIC 재할당 및 재시작

```

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 ->

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address     11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                    14) Enable Secure Shell (sshd)
6) Halt system                      15) Restore recent configuration
7) Ping host                        16) Restart PHP-FPM
8) Shell

Enter an option: █

```

```
Valid interfaces are:
```

```
em0      00:0c:29:1c:4b:c2   (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:1c:4b:cc   (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
```

```
Do VLANs need to be set up first?
```

```
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
```

```
Should VLANs be set up now [y n]? n
```

```
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.
```

```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a):
```

WAN 인터페이스: em0

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished):
```

LAN 인터페이스: em1

```
VMware Virtual Machine - Netgate Device ID: 5eeb79aa92e343adc071
```

```
*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***
```

```
WAN (wan) -> em0 ->
LAN (lan) -> em1 ->
```

- | | |
|---------------------------------------|----------------------------------|
| 0) Logout / Disconnect SSH | 9) pfTop |
| 1) Assign Interfaces | 10) Filter Logs |
| 2) Set interface(s) IP address | 11) Restart GUI |
| 3) Reset admin account and password | 12) PHP shell + pfSense tools |
| 4) Reset to factory defaults | 13) Update from console |
| 5) Reboot system | 14) Enable Secure Shell (sshd) |
| 6) Halt system | 15) Restore recent configuration |
| 7) Ping host | 16) Restart PHP-FPM |
| 8) Shell | |

```
Enter an option:
```

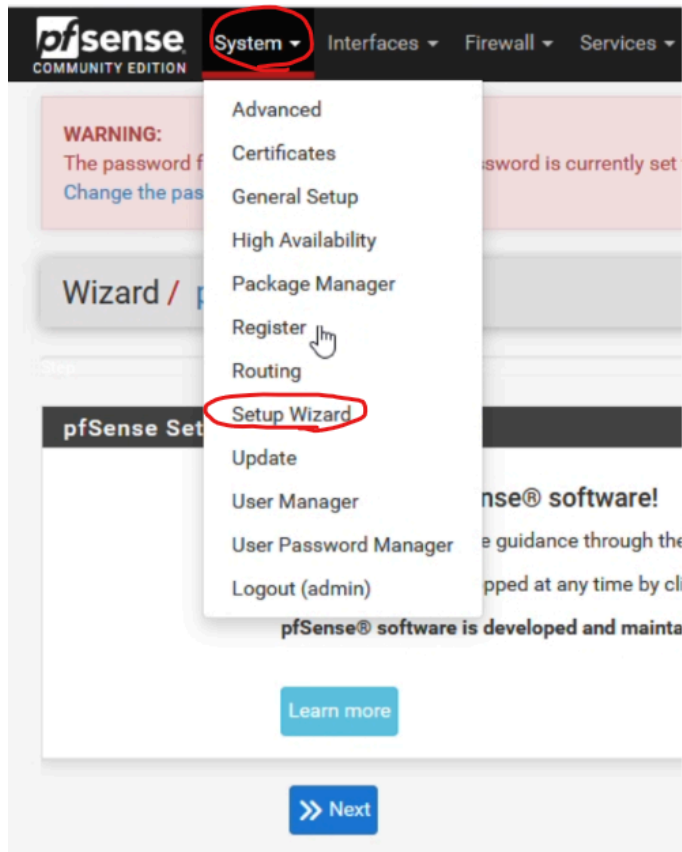
IP 설정 창 진입 (2번)

```
Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1)
Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 1.1.1.3/24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 1.1.1.1
Should this gateway be set as the default gateway? (y/n) y
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
> 
Do you want to enable the DHCP server on LAN? (y/n) n
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

IPS 구성: 1.1.1.2/24

IDS 구성: 1.1.1.3/24

이 후 네트워크 토폴로지 구성한 후에 Windows 10을 통한 웹 GUI 환경
진입



설정 마법사 시작

General Information

On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgfw

Domain
Domain name for the firewall.
Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices do not work correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'localdomain' are recommended.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries. To use the manually configured DNS servers below for client queries, visit Services > DNS > Resolver > Enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS ☐
Allow DNS servers to be overridden by DHCP/PPP on WAN

[Next](#)

pfSense
COMMUNITY EDITION

System

WARNING:
The password for this account is weak.
Change the password as soon as possible.

Wizard / pfSense Setup / Time Server Information

Step 3

Time Server Information

Time server hostname

Timezone

Asia/Sakhalin
Asia/Samarkand
Asia/Seoul
Asia/Shanghai
Asia/Singapore
Asia/Srednekolymsk
Asia/Taipei
Asia/Tashkent
Asia/Tbilisi
Asia/Tehran
Asia/Tel_Aviv
Asia/Thimbu
Asia/Thimphu
Asia/Tokyo
Etc/UTC

>> Next

RFC1918 Networks

Block RFC1918 Private Networks

☐ Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private use (172.16/12, 192.168/16) as well as loopback addresses (127/8). This WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks

☐ Block non-Internet routed networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for bogons. Bogons are prefixes that should never appear in the Internet routing table. Bogon addresses are not valid in any packets received.

>> Next

Wizard / pfSense Setup / Change admin Account Password

Step 6 of 9

Change admin Account Password

Change the password for the admin account.
This account is used to access the GUI, console (if protected), and SSH service (if enabled).

New admin Password

Confirm admin Password

>> Next

이후 설치 마법사 완료

IDS 초기 구성

pfSense COMMUNITY EDITION

System - **Interfaces** - Firewall - Services - VPN - Status - Diagnostics - Help

Interfaces / WAN

Assignments
WAN
LAN

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
Explicitly set speed and duplex mode for this interface.

WAN IP 형식: None

pfSense COMMUNITY EDITION

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

System /

Gateways Static Routes Gateway Groups

Gateways

Advanced
Certificates
General Setup
High Availability
Package Manager
Register
Routing
Setup Wizard
Update
User Manager
User Password Manager
Logout (admin)

Interface	Gateway	Monitor IP	Description	Actions
WAN	dynamic	dynamic	Interface WAN_DHCP6 Gateway	
WAN	dynamic	dynamic	Interface WAN_DHCP Gateway	
LAN	1.1.1.1	1.1.1.1	Interface lan Gateway	

Save + Add

System / Routing / Gateways

Gateways Static Routes Gateway Groups

Gateways

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
☒ WAN_DHCP6		WAN	dynamic	dynamic	Interface WAN_DHCP6 Gateway	
☒ WAN_DHCP		WAN	dynamic	dynamic	Interface WAN_DHCP Gateway	
☒ LANGW	Default (IPv4)	LAN	1.1.1.1	1.1.1.1	Interface lan Gateway	

Save + Add

LANGW 설정 제외하고 전부 삭제

System / Routing / Gateways / Edit

Edit Gateway

Disabled ☐ Disable this gateway
Set this option to disable this gateway without removing it from the list.

Interface
Choose which interface this gateway applies to.

Address Family
Choose the Internet Protocol this gateway uses.

Name
Gateway name

Gateway
Gateway IP address

Gateway Monitoring ☒ Disable Gateway Monitoring
This will consider this gateway as always being up.

Gateway Action ☐ Disable Gateway Monitoring Action
No action will be taken on gateway events. The gateway is always considered up.

Static route ☐ Do not add static route for gateway monitor IP address via the chosen interface
By default the firewall adds static routes for gateway monitor IP addresses to ensure traffic to the monitor IP address leaves via the correct interface. Enabling this checkbox overrides that behavior.

LANGW 설정에서 Gateway Monitoring 비활성화 옵션 체크

pfSense COMMUNITY EDITION

System - Interfaces - **Firewall** - Services - VPN - Status - Diagnostics - Help

Firewall / Rules / Floating

Floating WAN LAN

Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs

Rules (Drag to Change Order)

☐	States	Interfaces	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No floating rules are currently defined. Click the button to add a new rule.												

Firewall에서 모든 패킷 허용

Firewall / Rules / Floating / Edit

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Quick

☐ Apply the action immediately on match.

Set this option to apply this action to traffic that matches this rule immediately.

Interface

Any

WAN
LAN

Choose the interface(s) for this rule.

Direction

any

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

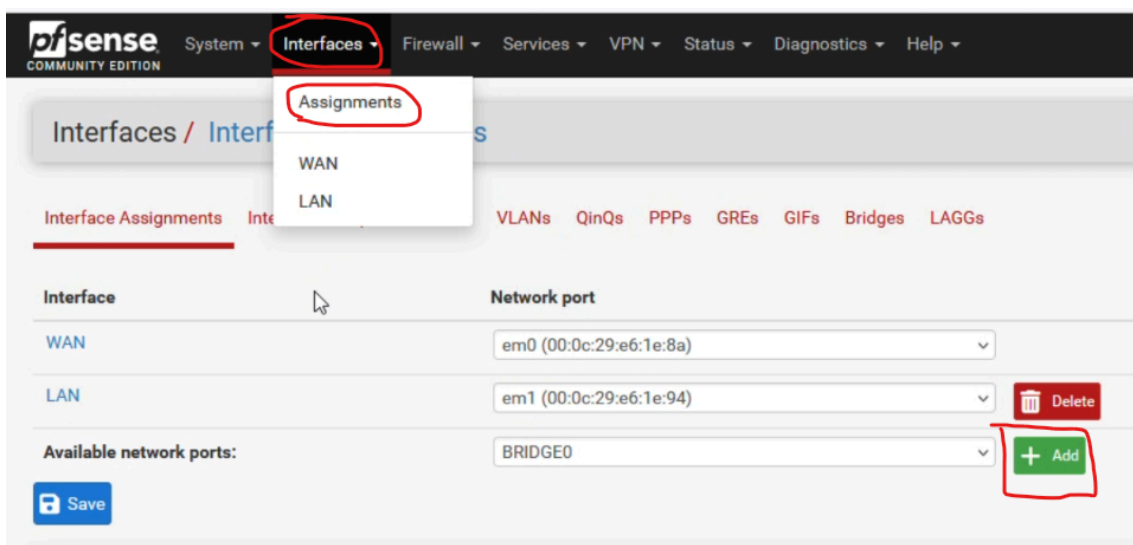
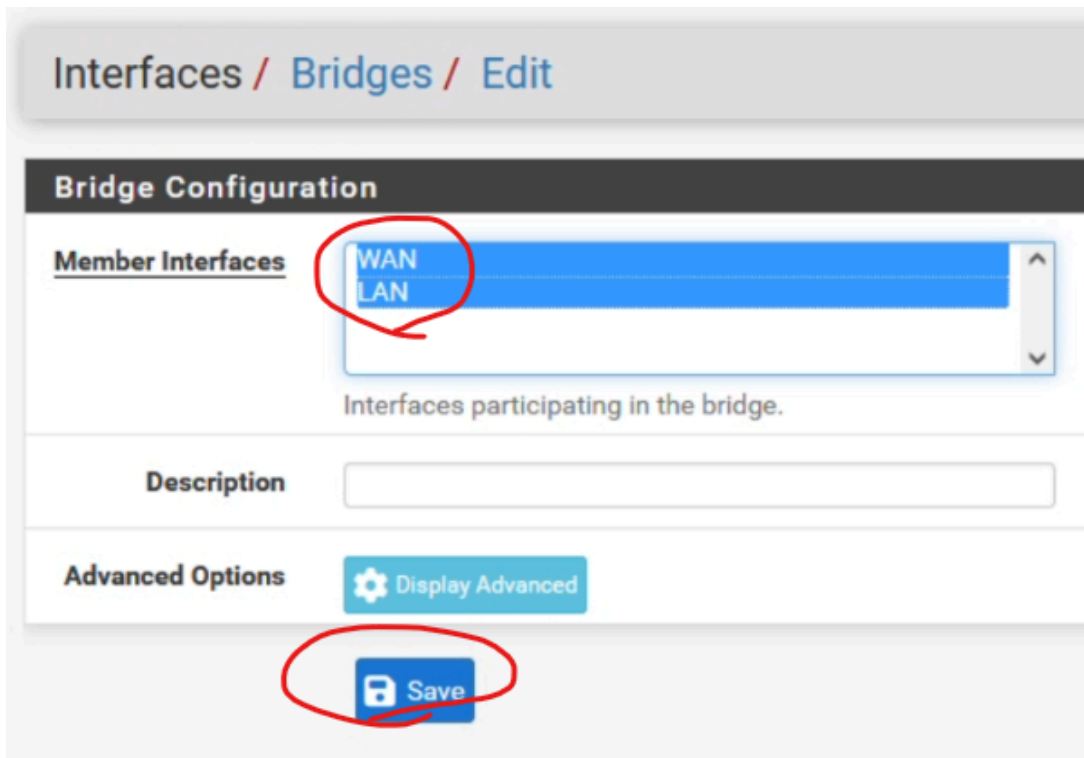
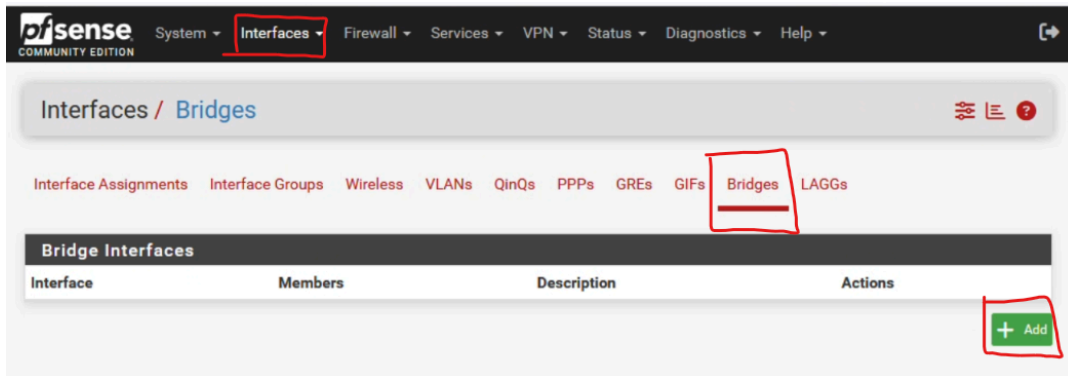
Protocol

Any

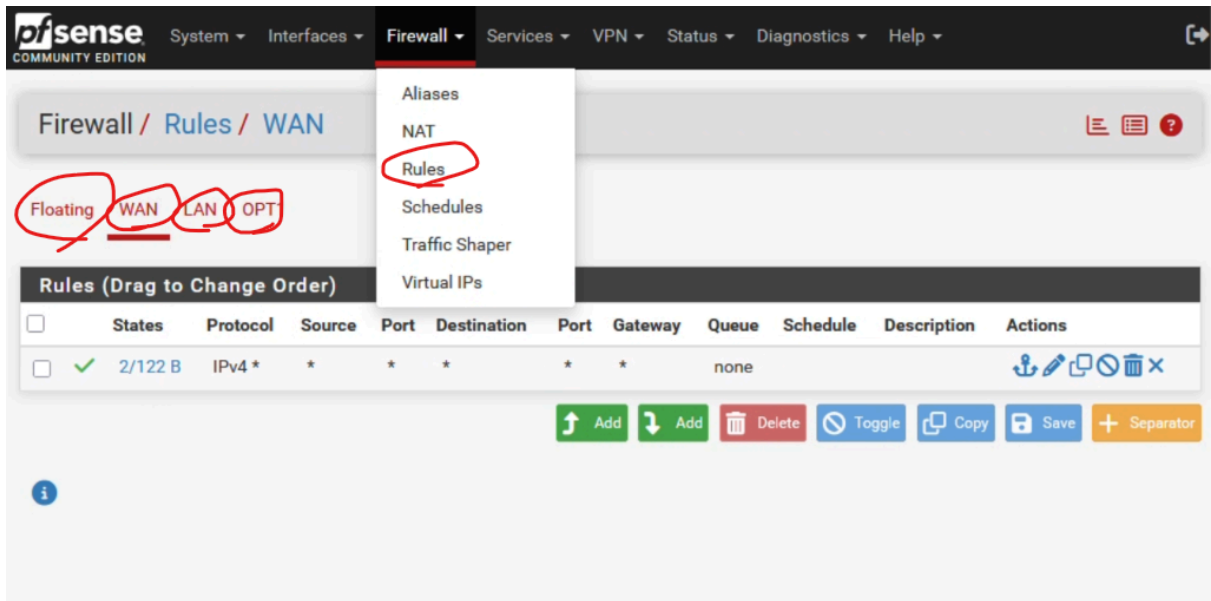
Choose which IP protocol this rule should match.

Floating, WAN, LAN 전부 동일하게 시행

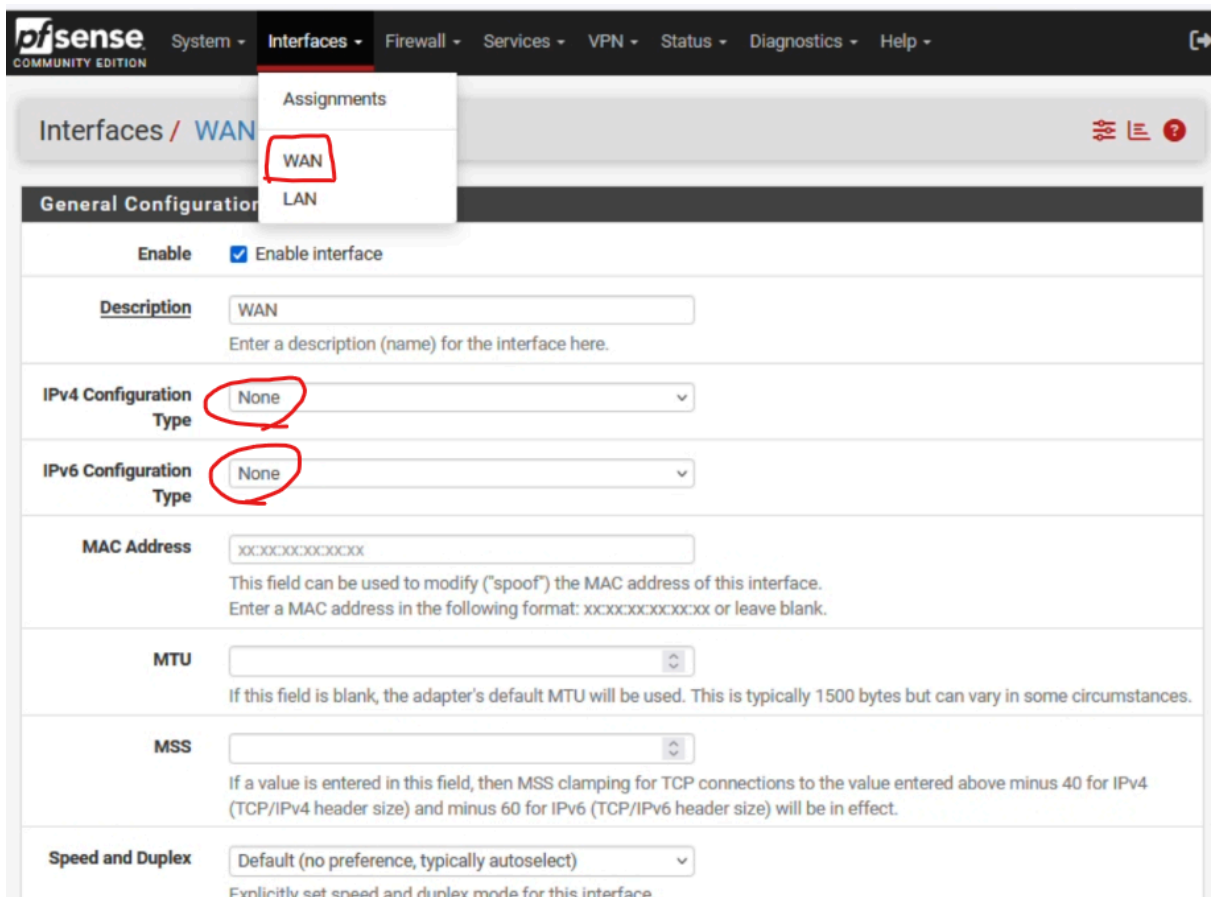
IPS 초기 구성



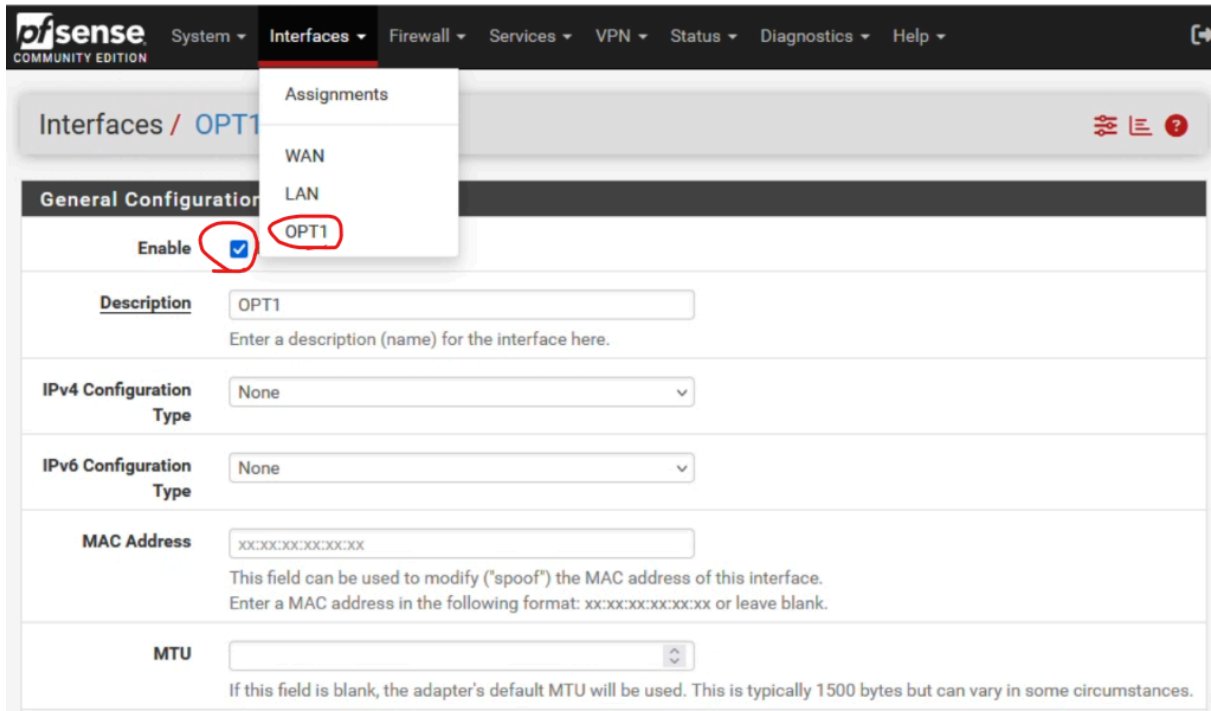
Bridge 인터페이스 생성 및 추가



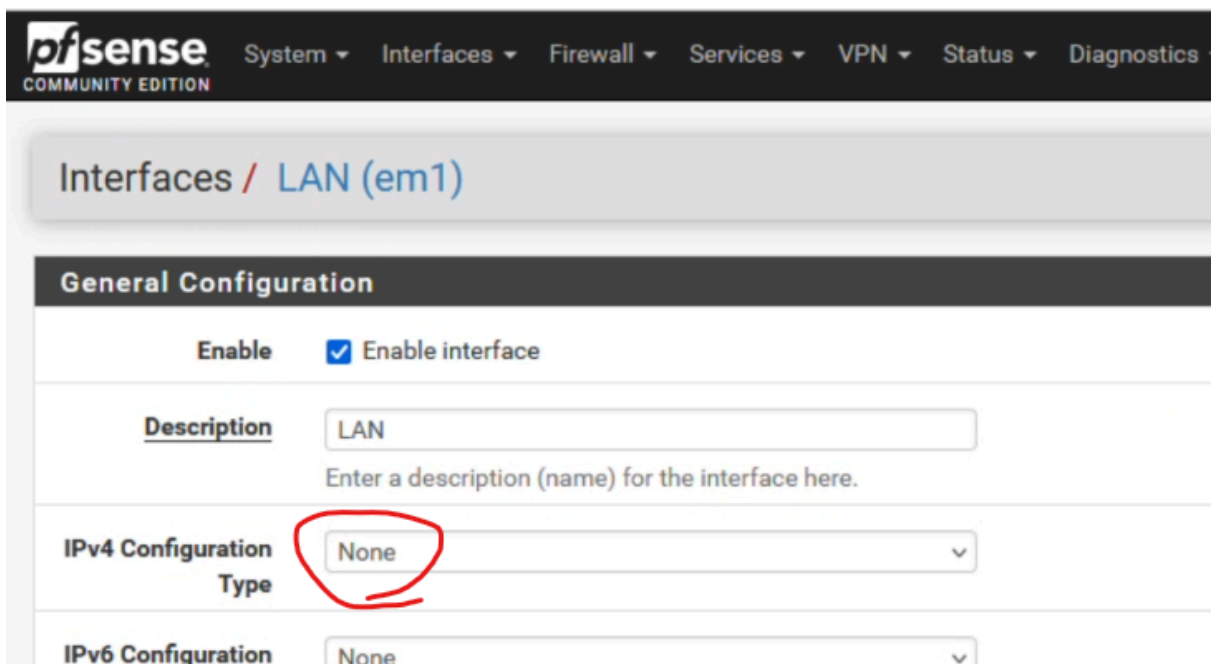
IDS와 동일하게 모든 인터페이스에 대한 방화벽 허용 설정



WAN IP 제거



OPT1 활성화



LAN의 IP 타입을 None으로 변경

모든 인터페이스에 IP가 없으므로 GUI에서 튕기고, 이 후 CLI에서 진행

Enter an option:

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: eec9a47822aca98d2373

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 ->
LAN (lan) -> em1 ->
OPT1 (opt1) -> bridge0 ->

0) Logout / Disconnect SSH

1) Assign Interfaces

2) Set interface(s) IP address

3) Reset admin account and password

4) Reset to factory defaults

5) Reboot system

6) Halt system

7) Ping host

8) Shell

9) pfTop

10) Filter Logs

11) Restart GUI

12) PHP shell + pfSense tools

13) Update from console

14) Enable Secure Shell (sshd)

15) Restore recent configuration

16) Restart PHP-FPM

Enter an option: █

모든 인터페이스에 IP가 없는 걸 확인

Enter an option: 2

Available interfaces:

1 - WAN (em0)

2 - LAN (em1)

3 - OPT1 (bridge0)

Enter the number of the interface you wish to configure: 3

Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address. Press <ENTER> for none:

> 1.1.1.2/24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:

> 1.1.1.1

Should this gateway be set as the default gateway? (y/n) y

```

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n
Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) n

Please wait while the changes are saved to OPT1...
Reloading filter...
Reloading routing configuration...

The IPv4 OPT1 address has been set to 1.1.1.2/24

```

브릿지 인터페이스에 IP 할당

System / Routing / Gateways

Gateways Static Routes Gateway Groups

Gateways							
	Name	Default	Interface	Gateway	Monitor IP	Description	Actions
☐	☒ WAN_DHCP		WAN	dynamic	dynamic	Interface WAN_DHCP Gateway	
☐	☒ WAN_DHCP6		WAN	dynamic	dynamic	Interface WAN_DHCP6 Gateway	
☐	☒ LANGW		LAN	1.1.1.1	1.1.1.1	Interface lan Gateway	
☐	☒ OPT1GW	Default (IPv4)	OPT1	1.1.1.1	1.1.1.1	Interface opt1 Gateway	

Save Add

OPT1GW 제외한 설정 전부 삭제

Edit Gateway

Disabled ☐ Disable this gateway
Set this option to disable this gateway without removing it from the list.

Interface
Choose which interface this gateway applies to.

Address Family
Choose the Internet Protocol this gateway uses.

Name
Gateway name

Gateway
Gateway IP address

Gateway Monitoring ☒ Disable Gateway Monitoring
This will consider this gateway as always being up.

Gateway Action ☐ Disable Gateway Monitoring Action
No action will be taken on gateway events. The gateway is always considered up.

Static route ☐ Do not add static route for gateway monitor IP address via the chosen interface
By default the firewall adds static routes for gateway monitor IP addresses to ensure traffic to the monitor IP address leaves via the correct interface. Enabling this checkbox overrides that behavior.

Gateway Monitoring 해제

pfSense **System** **Advanced** **System Tunables**

System Tunables

NOTE: The option is for use by advanced users only.

Tunable Name	Description	Value	Action
net.inet.ip.portrange_low	Low end of the port range	1024	
net.inet.tcp.blackbox	Do not send RST on segments to closed ports	2	
net.inet.udp.blackbox	Do not send port unreachable for refused connects	1	
net.inet.ip.random_id	Assign random ip_id values	1	
net.inet.tcp.drop_synfin	Drop TCP packets with SYN+FIN set	1	

+ New

System Tunables에서 옵션 추가

dev.igb.em0.fc

0

Flow Control (흐름 제어) 비활성화

dev.netmap.buf_size

2048

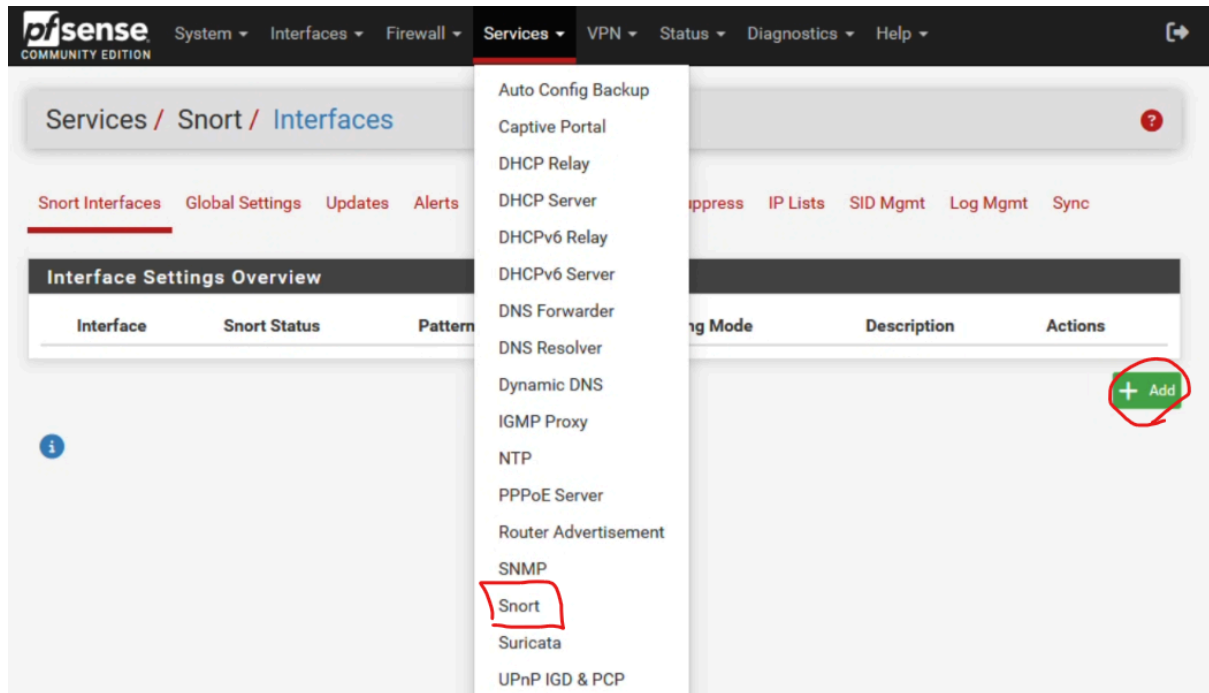
Netmap 버퍼 사이즈 조정

dev.igb.em0.eee_disabled

1

에너지 효율 이탈 방지

IDS snort 룰 테스트



Snort에서 WAN 인터페이스에 추가

General Settings

Enable ☒ Enable interface

Interface WAN (em0)
Choose the interface where this Snort instance will inspect traffic.

Description WAN
Enter a meaningful description here for your reference.

Snap Length 1518
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

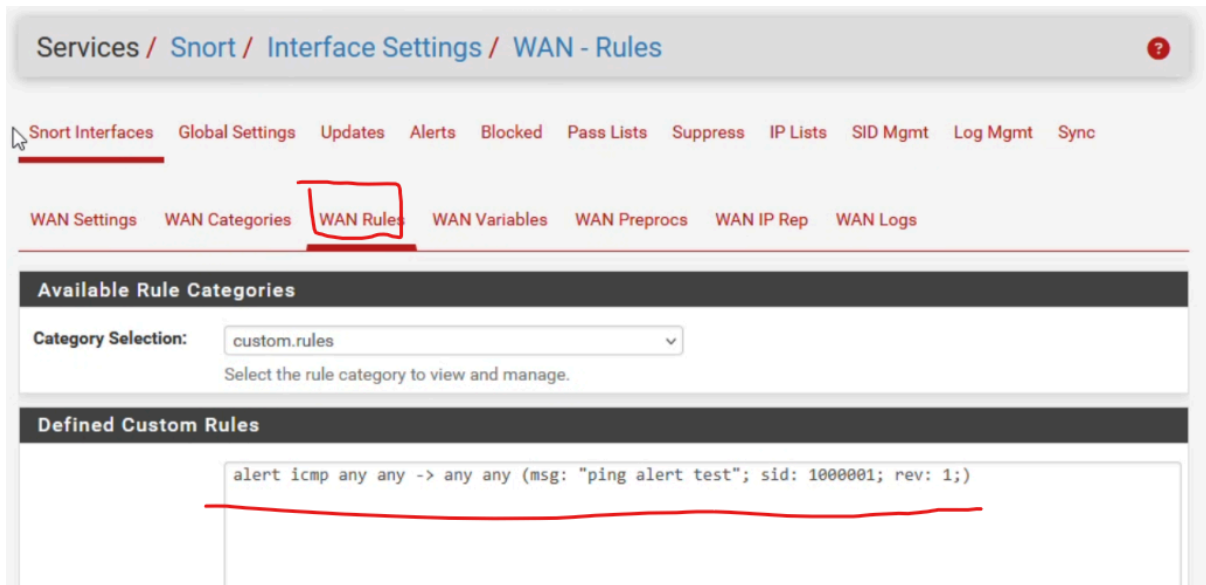
Send Alerts to System Log ☐ Snort will send Alerts to the firewall's system log. Default is Not Checked.

Enable Packet Captures ☒ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Packet Capture File Size 128
Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_em034348 is rotated and a new file opened.

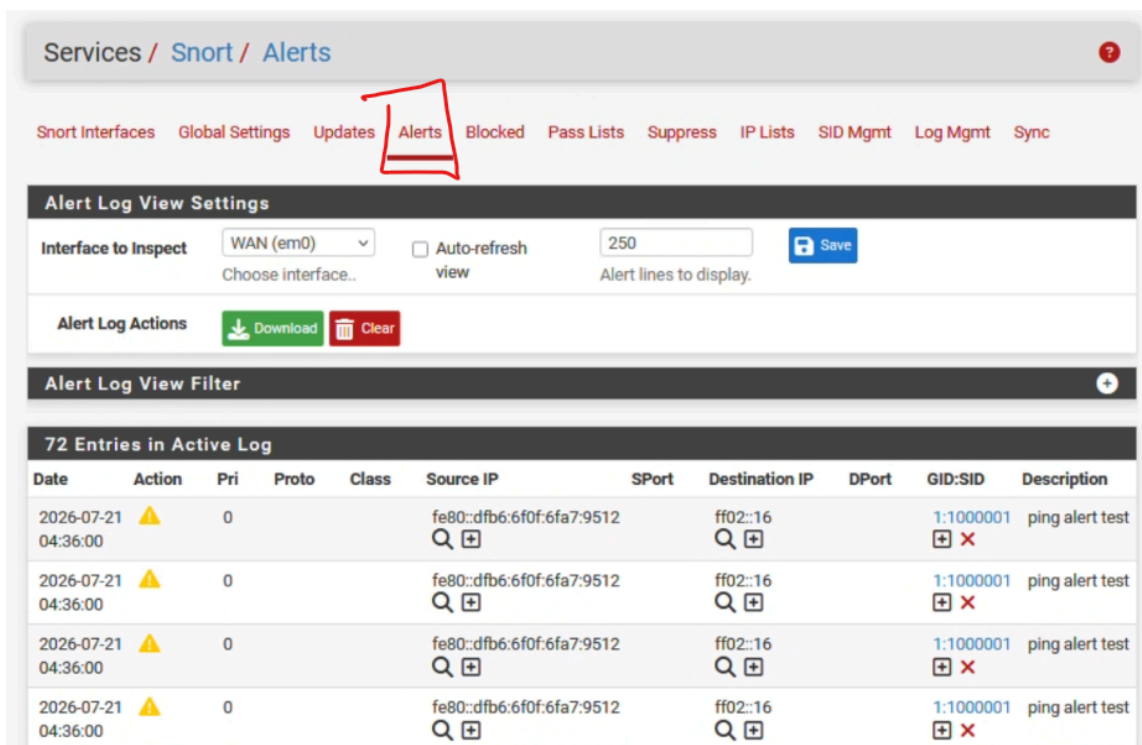
Enable Unified2 Logging ☐ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Packet Capture 옵션 활성화



alert test용 rule 입력

alert icmp any any -> any any (msg: "ping alert test"; sid: 1000001; rev: 1;)



정상 작동 시 Alerts 탭에서 노란색 아이콘으로 표시

[Snort Interfaces](#)[Global Settings](#)[Updates](#)[Alerts](#)[Blocked](#)[Pass Lists](#)[Suppress](#)[IP Lists](#)[SID Mgmt](#)[Log Mgmt](#)[Sync](#)

[WAN Settings](#)[WAN Categories](#)[WAN Rules](#)[WAN Variables](#)[WAN Preprocs](#)[WAN IP Rep](#)[WAN Logs](#)

Log File Selection

Log File to View

alert

Choose which log you want to view..

Log file contents

File successfully loaded.

Log File Path

/var/log/snort/snort_em06621/alert

Refresh

Log Contents

07/21/26-04:23:30.475608 ,1,1000001,1,"ping alert test",,fe80::20c:29ff:fe04:aa65,,ff02::2,,0,,0,alert,Allow
07/21/26-04:23:32.909331 ,1,1000001,1,"ping alert test",ICMP,2.1.1.2,,1.1.1.4,,40270,,0,alert,Allow
07/21/26-04:23:32.925167 ,1,1000001,1,"ping alert test",ICMP,1.1.1.4,,2.1.1.2,,21356,,0,alert,Allow
07/21/26-04:23:33.910604 ,1,1000001,1,"ping alert test",ICMP,2.1.1.2,,1.1.1.4,,40271,,0,alert,Allow
07/21/26-04:23:33.910791 ,1,1000001,1,"ping alert test",ICMP,1.1.1.4,,2.1.1.2,,22006,,0,alert,Allow
07/21/26-04:23:34.912310 ,1,1000001,1,"ping alert test",ICMP,2.1.1.2,,1.1.1.4,,40449,,0,alert,Allow
07/21/26-04:23:34.912495 ,1,1000001,1,"ping alert test",ICMP,1.1.1.4,,2.1.1.2,,23006,,0,alert,Allow
07/21/26-04:23:35.918721 ,1,1000001,1,"ping alert test",ICMP,2.1.1.2,,1.1.1.4,,40688,,0,alert,Allow
07/21/26-04:23:35.918905 ,1,1000001,1,"ping alert test",ICMP,1.1.1.4,,2.1.1.2,,23824,,0,alert,Allow

기본 설정: alert_fast

IPS snort 룰 테스트

Services / Snort / Interfaces ?

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
☐ WAN (em0)	✔ ↺	AC-BNFA	INLINE IPS	WAN	✎ 📄 🗑️

+ Add Delete

i

WAN Settings

General Settings

Enable ☒ Enable interface

Interface WAN (em0) ▼
Choose the interface where this Snort instance will inspect traffic.

Description WAN
Enter a meaningful description here for your reference.

Snap Length 1518 ▼
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log ☐ Snort will send Alerts to the firewall's system log. Default is Not Checked.

Enable Packet Captures ☒ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Packet Capture File Size 128 ▼
Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_em021447 is rotated and a new file opened.

Block Settings

Block Offenders ☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode Inline Mode ▼
Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

IDS와 다르게 Block Offenders 옵션을 키고 Inline Mode 활성화

WARNING! IPS inline mode requires that Hardware Checksum Offloading, Hardware TCP Segmentation Offloading and Hardware Large Receive Offloading all be disabled for proper operation. This firewall currently has one or more of these Offloading settings NOT disabled. Visit the [System > Advanced > Networking](#) tab and ensure all three of these Offloading settings are disabled.

Network Interfaces

Hardware Checksum Offloading	☒ Disable hardware checksum offload Checking this option will disable hardware checksum offloading. Checksum offloading is broken in some hardware, particularly some Realtek cards. Rarely, drivers may have problems with checksum offloading and some specific NICs. This will take effect after a machine reboot or re-configure of each interface.
Hardware TCP Segmentation Offloading	☒ Disable hardware TCP segmentation offload Checking this option will disable hardware TCP segmentation offloading (TSO, TSO4, TSO6). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs. This will take effect after a machine reboot or re-configure of each interface.
Hardware Large Receive Offloading	☒ Disable hardware large receive offload Checking this option will disable hardware large receive offloading (LRO). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs. This will take effect after a machine reboot or re-configure of each interface.
hn ALTQ support	☒ Enable the ALTQ support for hn NICs. Checking this option will enable the ALTQ support for hn NICs. The ALTQ support disables the multiqueue API and may reduce the system capability to handle traffic. This will take effect after a machine reboot.

이후 재부팅

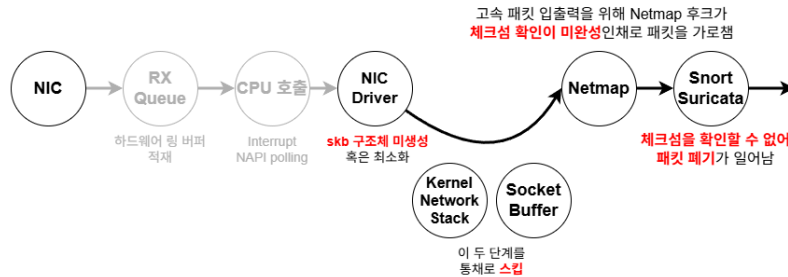
```
[2.8.1-RELEASE][root@pfSense.home.arpal]/root: tail -f /var/log/system.log
Jul 20 16:36:54 pfSense kernel: 413.886635 [4308] netmap_transmit          em0
drop mbuf that needs checksum offload
Jul 20 16:38:53 pfSense kernel: 533.711229 [4308] netmap_transmit          em0
drop mbuf that needs checksum offload
Jul 20 16:40:44 pfSense kernel: 644.810954 [4308] netmap_transmit          em0
drop mbuf that needs checksum offload
Jul 20 16:42:54 pfSense kernel: 774.321241 [4308] netmap_transmit          em0
drop mbuf that needs checksum offload
Jul 20 16:44:50 pfSense kernel: 889.981168 [4308] netmap_transmit          em0
drop mbuf that needs checksum offload
Jul 20 16:46:41 pfSense kernel: 001.770893 [4308] netmap_transmit          em0
drop mbuf that needs checksum offload
Jul 20 16:48:50 pfSense kernel: 130.219653 [4308] netmap_transmit          em0
drop mbuf that needs checksum offload
Jul 21 01:49:42 pfSense login[5890]: login on ttyv0 as root
Jul 20 16:50:47 pfSense kernel: 246.961683 [4308] netmap_transmit          em0
drop mbuf that needs checksum offload
Jul 20 16:52:45 pfSense kernel: 365.323922 [4308] netmap_transmit          em0
drop mbuf that needs checksum offload
```

/var/log/system.log

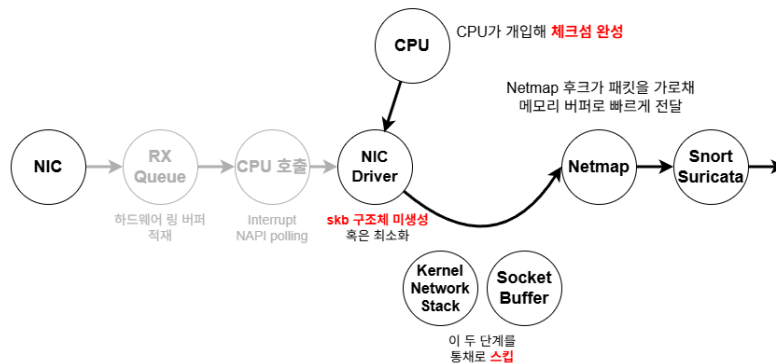
일반적인 환경
Netmap 비활성화 시
checksum offload: **on**



IPS Inline 구성
Netmap 활성화 시
checksum offload: **on**



IPS Inline 구성
Netmap 활성화 시
checksum offload: **off**



checksum offload가 켜져있으면 네트워크 카드가 나중에 직접 처리하려고 미루고, netmap 고속 패킷 프레임워크를 사용하는 snort는 미완성 패킷을 읽어들이지 못해 강제로 drop시킴. 이 옵션을 꺼 줌으로써 CPU가 직접 패킷을 처리해서 snort에게 던지게 만들어야함.

```
cat /usr/local/etc/snort/snort_em*/snort.conf | grep daq
```

```
cat /usr/local/etc/snort/snort_6621_em0/snort.conf | grep daq
```

Services / Snort / Interface Settings / WAN - Rules

Snort InterfacesGlobal SettingsUpdatesAlertsBlockedPass ListsSuppressIP ListsSID MgmtLog MgmtSync

WAN SettingsWAN CategoriesWAN RulesWAN VariablesWAN PreprocsWAN IP RepWAN Logs

Available Rule Categories

Category Selection: custom.rules

Select the rule category to view and manage.

Defined Custom Rules

drop icmp any any -> any any (msg: "ping alert test"; sid: 1000001; rev: 1;)

Services / Snort / Alerts

Snort InterfacesGlobal SettingsUpdatesAlertsBlockedPass ListsSuppressIP ListsSID MgmtLog MgmtSync

Alert Log View Settings

Interface to Inspect WAN (em0)

Choose interface..

Auto-refresh view

Alert lines to display. 250

Save

Alert Log Actions

Download

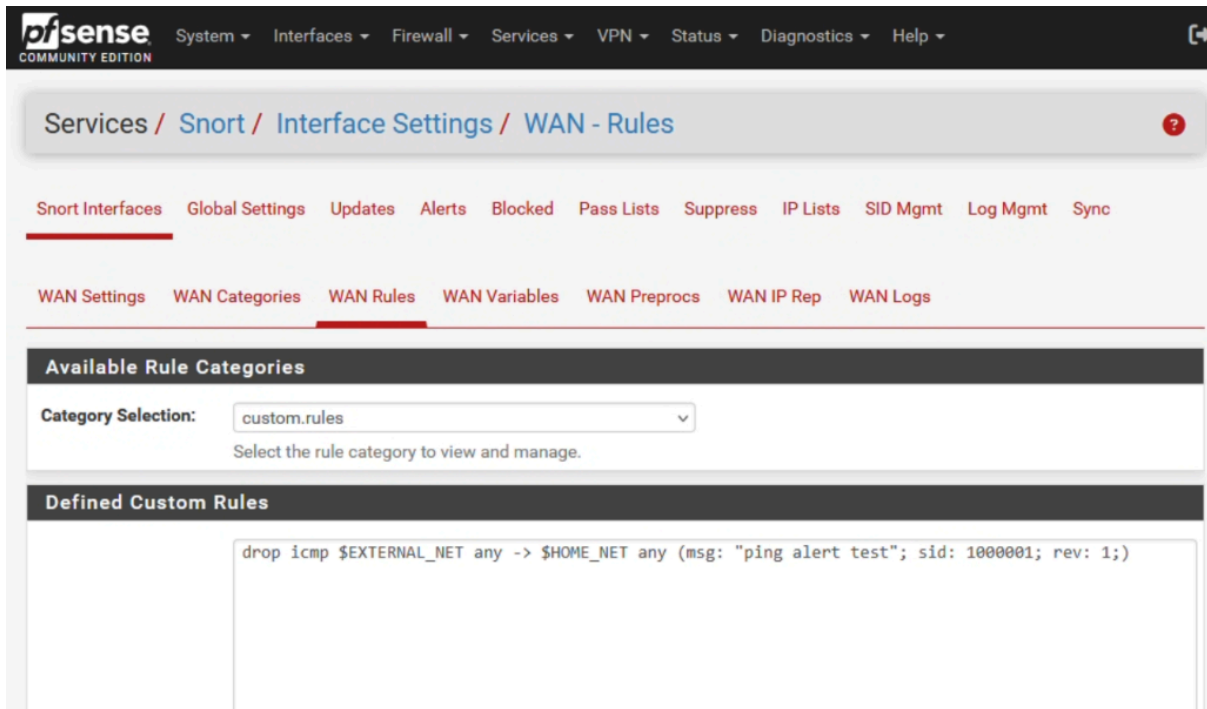
Clear

Alert Log View Filter

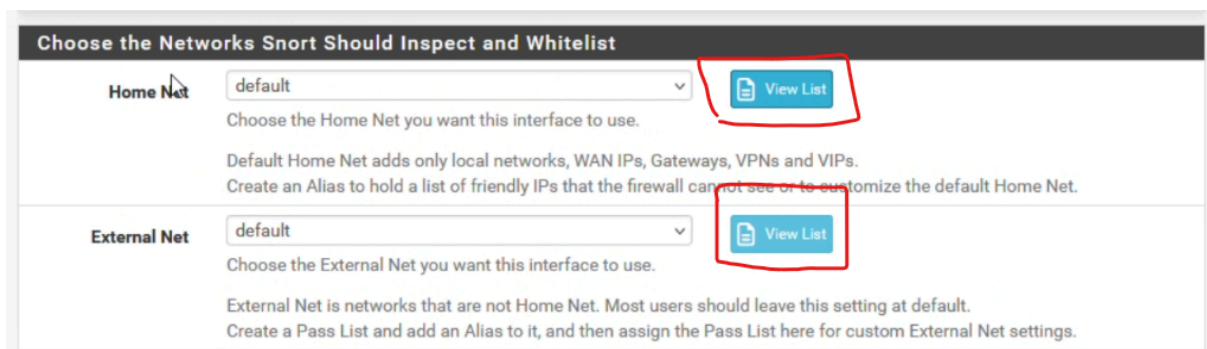
6 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2026-07-21 04:54:49		0	ICMP		2.1.1.2		1.1.1.4		1:1000001	ping alert test
2026-07-21 04:54:48		0	ICMP		2.1.1.2		1.1.1.4		1:1000001	ping alert test
2026-07-21 04:54:47		0	ICMP		2.1.1.2		1.1.1.4		1:1000001	ping alert test

HOME_NET, EXTERNAL_NET



pfSense 방화벽의 기본 변수 자동 정의 기능에 의해 외부와 내부 변수가 정상적으로 작동.



Java-attack

```
drop tcp any any -> any any (msg:"DVWA JS Logic Bypass - URI Path Check";  
flow:established,to_server; content:"/vulnerabilities/javascript/"; http_uri;  
sid:2005001; rev:1;)
```

```
drop tcp any any -> any any (msg:"DVWA JS Logic Bypass - Phrase Check";  
flow:established,to_server; content:"phrase=success"; nocase; sid:2005002;  
rev:1;)
```

```
drop tcp any any -> any any (msg:"DVWA JS Logic Bypass - Token Check";  
flow:established,to_server;  
content:"token=38581812b435834ebf84ebcc2c6424d6"; nocase; sid:2005003;  
rev:1;)
```

```
drop tcp any any -> any any (msg:"DVWA JS Logic Bypass - URI Path Check (IPS  
Fix)"; flow:established,to_server; content:"/vulnerabilities/javascript/"; nocase;  
sid:2005001; rev:2;)
```

1번이 IPS 모드에서 잘 안 되는데, snort 내부 http 인스펙터가 TCP 패킷들을 조립하고
규격에 맞게 파싱하고 정규화
http를 제거하면 잘 되는데, 패킷 페이로드 Raw data를 검사하기 때문

명령어 모음

ip.addr != 1.1.1.2 and ip.addr != 1.1.1.3 and not mdns and not llmnr and not nbns
and not dhcp and not browser and not igmp

ping test

```
alert icmp any any -> any any (msg: "ping alert test"; sid: 1000001; rev: 1;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg: "ping alert test"; sid:
1000001; rev: 1;
)
```

Javascript 테스트

```
alert tcp any any -> any any (msg:"DVWA JavaScript Logic Bypass";
flow:established,to_server; content:"/vulnerabilities/javascript/"; http_uri;
content:"phrase=success"; nocase;
content:"token=38581812b435834ebf84ebcc2c6424d6"; nocase; sid:2005001;
rev:1;)
```

```
alert tcp any any -> any any (msg:"DVWA JavaScript Logic Bypass";
flow:established,to_server;
content:"token=38581812b435834ebf84ebcc2c6424d6"; nocase; sid:2005001;
rev:1;)
```

1 x

```
drop tcp any any -> any any (msg:"DVWA JS Logic Bypass - URI Path Check";  
flow:established,to_server; content:"/vulnerabilities/javascript/"; http_uri;  
sid:2005001; rev:1;)
```

2 0

```
drop tcp any any -> any any (msg:"DVWA JS Logic Bypass - Phrase Check";  
flow:established,to_server; content:"phrase=success"; nocase; sid:2005002;  
rev:1;)
```

3 0

```
drop tcp any any -> any any (msg:"DVWA JS Logic Bypass - Token Check";  
flow:established,to_server;  
content:"token=38581812b435834ebf84ebcc2c6424d6"; nocase; sid:2005003;  
rev:1;)
```

fix

```
drop tcp any any -> any any (msg:"DVWA JS Logic Bypass - URI Path Check (IPS  
Fix)"; flow:established,to_server; content:"/vulnerabilities/javascript/"; nocase;  
sid:2005001; rev:2;)
```

```
nmap -v -sS 1.1.1.0/24
```

```
alert tcp any any -> any any (msg:"NMAP SYN Scan Detected"; flags:S;  
sid:3000001; rev:1;)
```

`nmap -sU, threshold`

threshold 타입 3가지:

type threshold

- 지정한 시간 (second) 동안 트래픽이 몰릴 때 설정한 횟수 (count)를 넘을 때 마다 알림 발생
- count 10, second 60이면, 60초동안 10번째 패킷 이후로 계속 알림

type limit

- threshold와 반대로, count 만큼 알림 발생시키고 남은 시간동안 무시
- 로그 폭탄을 막기에 좋음

type both

- limit과 동일하게 작동하되, 주기 내 여러 번 발생하면 간격에 맞춰 제한적으로 알림을 남김

UDP 스캔

`nmap -v -sU 1.1.1.4`

빠른 UDP 스캔

`nmap -v -sU -T4 -F 1.1.1.4`

`drop udp any any -> any any (msg:"NMAP UDP Scan Flood Detected"; threshold: type threshold, track by_src, count 50, seconds 2; sid:3000011; rev:1;)`

track by_src가 없으면 전체 UDP가 집계되어 마비 위험성이 있음

track by_dst: ddos 방어에 제한적으로 사용