Assignment 3:  
Security Servers and pfSense

*Pod #5*

*ISEC2700*

*10/09/2024*

Table of Contents

[Task 3 2](#_Toc179891241)

WAN (em0) Config: DHCP 192.168.208.135/24

LAN (em1) Config: Static 192.168.208.100/24

# Task 3

* Because we are doing this in a virtual network, **uncheck** “Block RFC1918 private networks” and “Block bogon networks”
  + **Stop**. Take a minute to research what these settings mean and add it to your Glossary in your document and be prepared to explain then during demo.

Leaving these settings on assumes that traffic for the server will be coming directly from the internet as they block traffic from private addresses to lighten server load. Since all our traffic to this server will be coming from VMs, we can safely disable it.

* **Question 1.** What does Snort VRT do and why are we enabling it?

Snort is an Intrusion Prevention System we are using to set up a level of security monitoring on our servers and to prevent any potential attacks. (Snort)

* **Question 2.** What is OpenAppID and what is the difference between these two options (OpenAppID and AppID Open Text rules) and why did we enable both?

OpenAppID and AppID OpenText are both forms of Application Detection. OpenAppID was developed by the Snort community to create custom application identification rules, while AppID OpenText was designed specifically to work with OpenText’s products. We enabled both because we are working within Snort and will be using OpenText plug-ins.

* **Question 3**. What does the IPS Policy do and why are we selecting it?

This setting changes Snort to look at a predefined list of attacks as opposed to letting the server administrator input their own set of rules and traffic to block and/or report.

* **Question 4.** What does the IPS Policy Selection do and why did we set our selection to “Security”?

This changes how strict Snort will behave. It determines what kind of traffic it will report and block from Connectivity blocking most major threats to Max-Detect catching and blocking everything. We chose Security as it will show us more reports while not blocking everything outright like Max-Detect would.

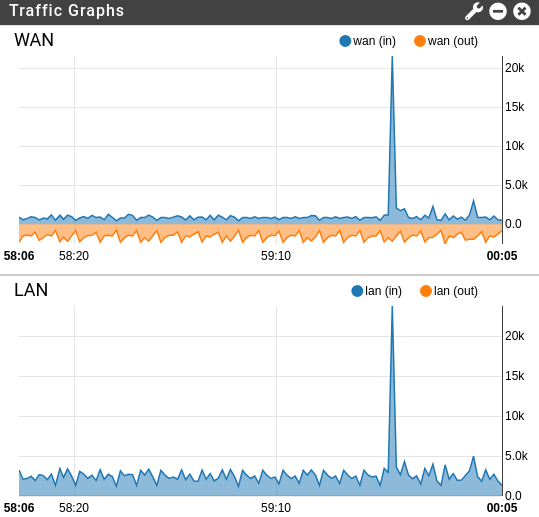
* **Question 5.** What are the 7 logs are available in your Log Mgmt/Log Size and Retention Limits? What do they capture and how do you access the logs?
  + - **alert** logs Snort alerts and event details
    - **snort\_xxxx.u2** logs Snort alerts and event details in Unified2 binary log format
    - **appid-alerts** logs Application ID alerts
    - **app-stats** logs Application ID statistics
    - **event pcaps** logs Snort alert related packet captures
    - **sid\_changes** logs SID changes made by SID Mgmt conf files
    - **stats** logs Snort performance statistics.

All of these logs are visible in /var/log/snort

* **Question 6.** What is “Talos” and what is it used for and who uses it?

Talos is the Talos Intelligence Group, a branch of Cisco who research threats to help keep Snort up to date. Network Administrators using Snort on their servers would actively be using Talos any time they are using their IPS rules.

* **Question 7.**When we view our PfSense Dashboard we can see several different pieces of information under System Information that help us management our security server. Other then CPU Usage, identify 5 other pieces of information and explain why it is helpful/important to have this data.
  + - **Version** is important to see front and center to know whenever an update is available and to verify that you are running the latest software.
    - **Current date/time** helps verify that Chrony is running and configured to stop any desync issues
    - **DNS Server** is helpful to have displayed in case of any connectivity issues with host machines.
    - **Name** displays the servers NetBIOS/FQDN in full, helpful for double-checking domain connections.
    - **Memory usage** is helpful in a similar way to CPU, to make sure the server is not under a heavy load or to help diagnose speed or connection issues.
* **Question 8.**While watching your Traffic Graph your should see at least 2 or more IPs. Record the 2 IPs from your graph and identify the device they reference. Include a screenshot of your Graph captures and IP capture.



*NIC 1 and NIC 2*