Robert Carpenter
github.com/robertmcarpenter
Wed December 11th 2024

Lab 6.3.4: Configuring an Intrusion Detection System on a pfSense Security Appliance

From TestOut CompTIA Security+ Course

In this lab I will be configuring an Intrusion Detection System using an Open Source package called Snort, within a pfSense Security Appliance environment.

The scenario for this lab is as follows:

“You work as the IT security administrator for a small corporate network. In an effort to protect your network against security threats and hackers, you have added Snort to pfSense. With Snort already installed, you need to configure rules and settings and then assign Snort to the desired interface.

In this lab, your task is to use pfSense's Snort to complete the following:

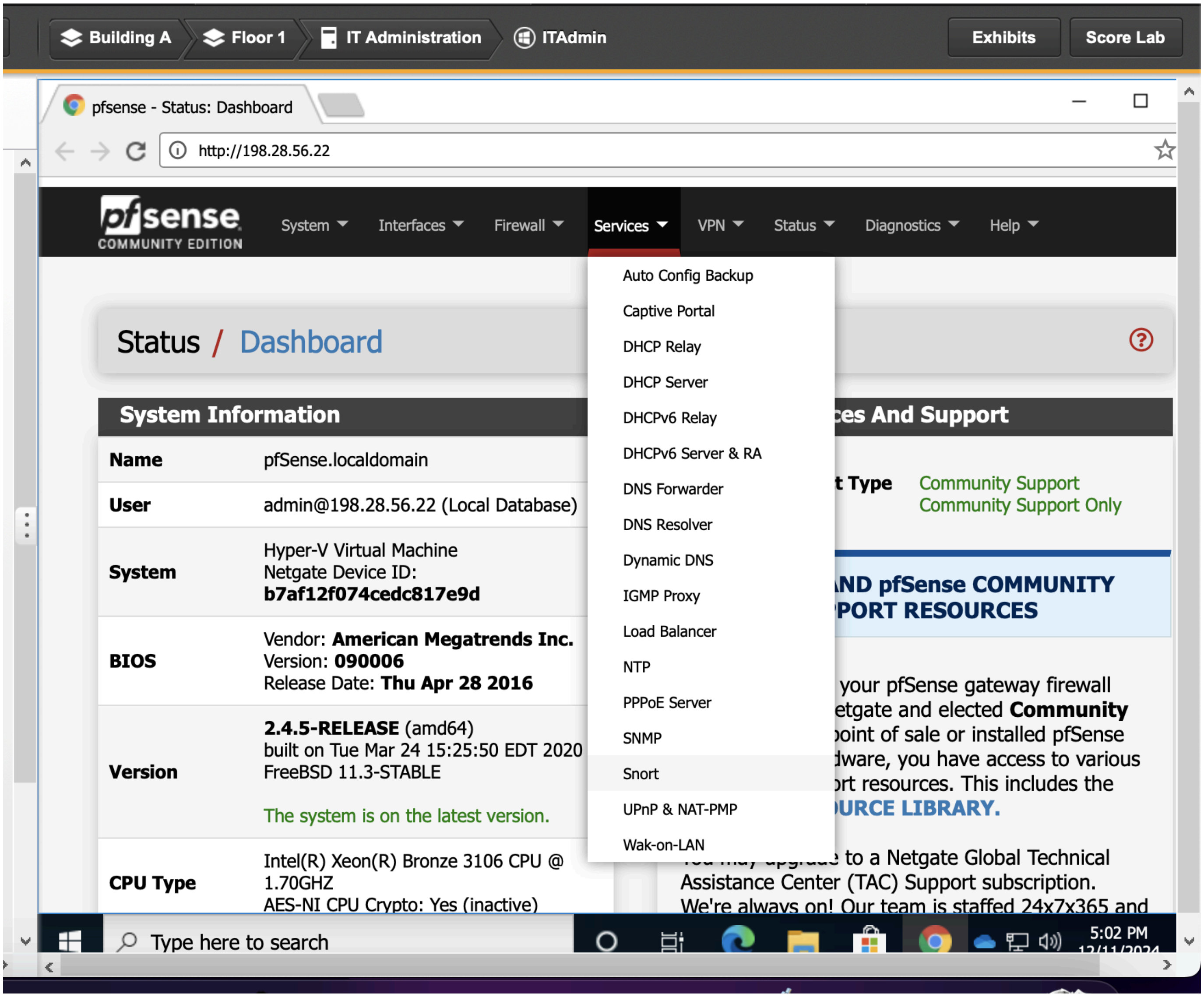
Sign in to pfSense using the following:

- Username: **admin**
- Password: **P@ssw0rd** (zero)
- Enable the downloading of the following:
  - Snort free registered User rules
    - Oinkmaster Code: **359d00c0e75a37a4dbd70757745c5c5dg85aa**
  - Snort GPLv2 Community rules
  - Emerging Threats Open rules
  - Sourcefire OpenAppID detectors
  - APPID Open rules
- Configure rule updates to happen once a day at 1:00 a.m.
  - Hide any deprecated rules.
- Block offending hosts for 1 hour.
- Send all alerts to the system log when the Snort starts and stops.
- Assign Snort to the WAN interface using a description of **WANSnort**.
  - Include:
    - Sending alerts to the system log
    - Automatically blocking hosts that generate a Snort alert

Robert Carpenter
github.com/robertmcarpenter
Wed December 11th 2024

- Start Snort on the WAN interface.”

I will start by logging in to the pfSense security Appliance with the credentials applied. Once I am in , I will navigate over to the Package Installer within the pfSense GUI environment.



Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@198.28.56.22 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: **b7af12f074cedc817e9d**
BIOS	Vendor: **American Megatrends Inc.** Version: **090006** Release Date: **Thu Apr 28 2016**
Version	**2.4.5-RELEASE** (amd64) built on Tue Mar 24 15:25:50 EDT 2020 FreeBSD 11.3-STABLE The system is on the latest version.
CPU Type	Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHZ AES-NI CPU Crypto: Yes (inactive)

ces And Support

t Type Community Support
Community Support Only

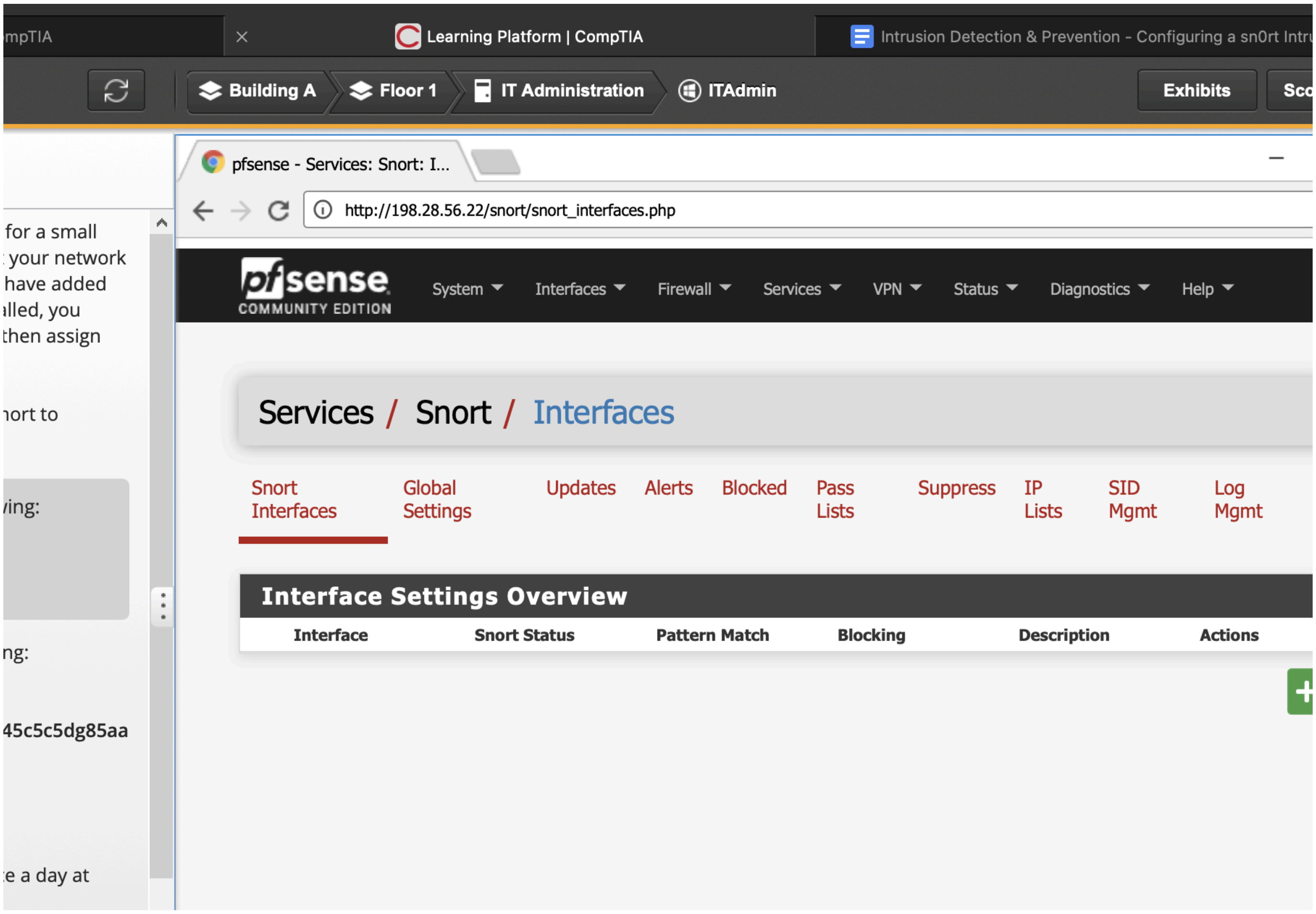
ND pfSense COMMUNITY
PORT RESOURCES

your pfSense gateway firewall
etgate and elected **Community**
point of sale or installed pfSense
dware, you have access to various
ort resources. This includes the
URCE LIBRARY.

to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and

In **Services > Snort** I’ll click it to open the configuration.

Robert Carpenter
github.com/robertmcarpenter
Wed December 11th 2024



Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking	Description	Actions

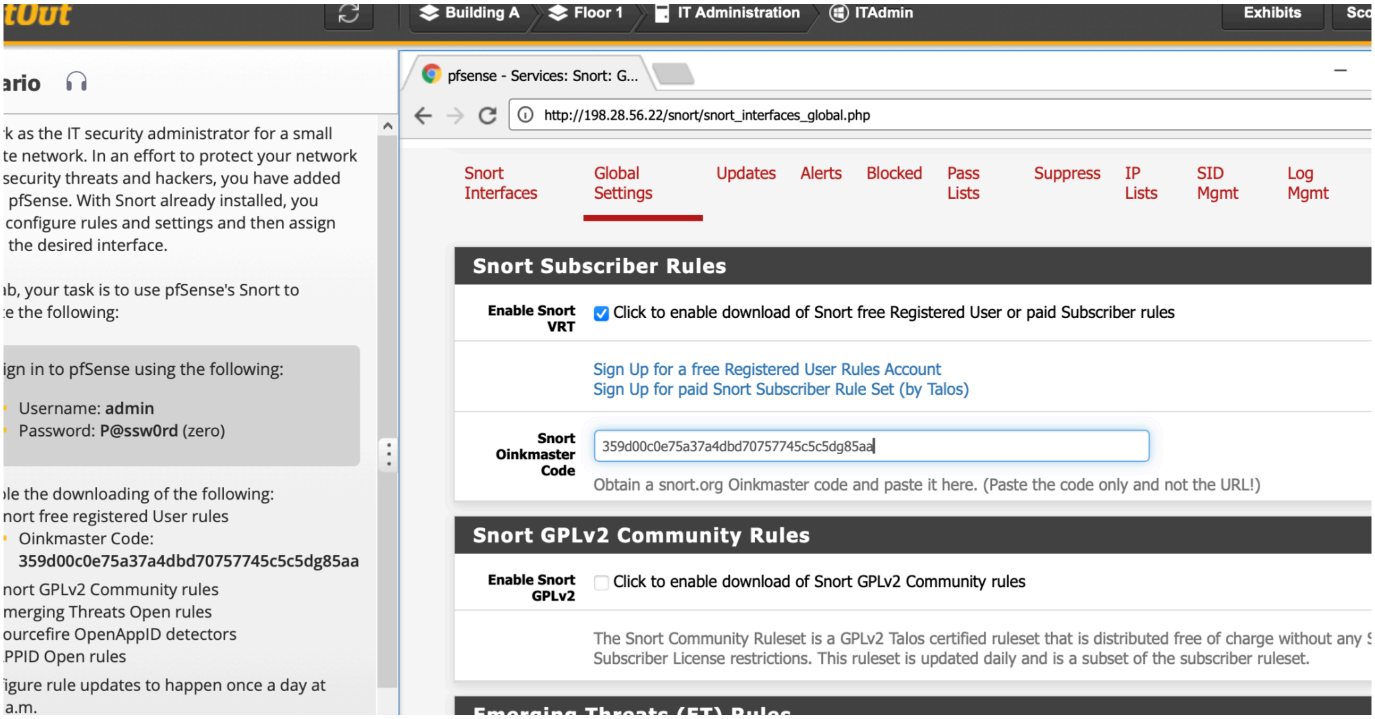
Once on the Snort Service page, I'll click the **Global Settings** breadcrumb on the menu to open the general configuration.

My First task in this lab is to set the following settings:

- Enable the downloading of the following:
  - Snort free registered User rules
    - Oinkmaster Code: **359d00c0e75a37a4dbd70757745c5c5dg85aa**
  - Snort GPLv2 Community rules
  - Emerging Threats Open rules
  - Sourcefire OpenAppID detectors
  - APPID Open rules

Robert Carpenter
github.com/robertmcarpenter
Wed December 11th 2024

Note that even though Snort is open source, they offer a paid subscription to update rules 30 days ahead of users on the GPL license. Since we are setting up Snort for the first time, we need to download the **Free User Rules**.



ario

k as the IT security administrator for a small te network. In an effort to protect your network security threats and hackers, you have added pfSense. With Snort already installed, you configure rules and settings and then assign the desired interface.

ab, your task is to use pfSense's Snort to e the following:

ign in to pfSense using the following:

- Username: **admin**
- Password: **P@ssw0rd** (zero)

le the downloading of the following:
nort free registered User rules
- Oinkmaster Code: **359d00c0e75a37a4dbd70757745c5c5dg85aa**

nort GPLv2 Community rules
merging Threats Open rules
ourcefire OpenAppID detectors
PPID Open rules
igure rule updates to happen once a day at a.m.

http://198.28.56.22/snort/snort_interfaces_global.php

Snort Subscriber Rules

Enable Snort VRT ☑ Click to enable download of Snort free Registered User or paid Subscriber rules

Sign Up for a free Registered User Rules Account
Sign Up for paid Snort Subscriber Rule Set (by Talos)

Snort Oinkmaster Code 359d00c0e75a37a4dbd70757745c5c5dg85aa

Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

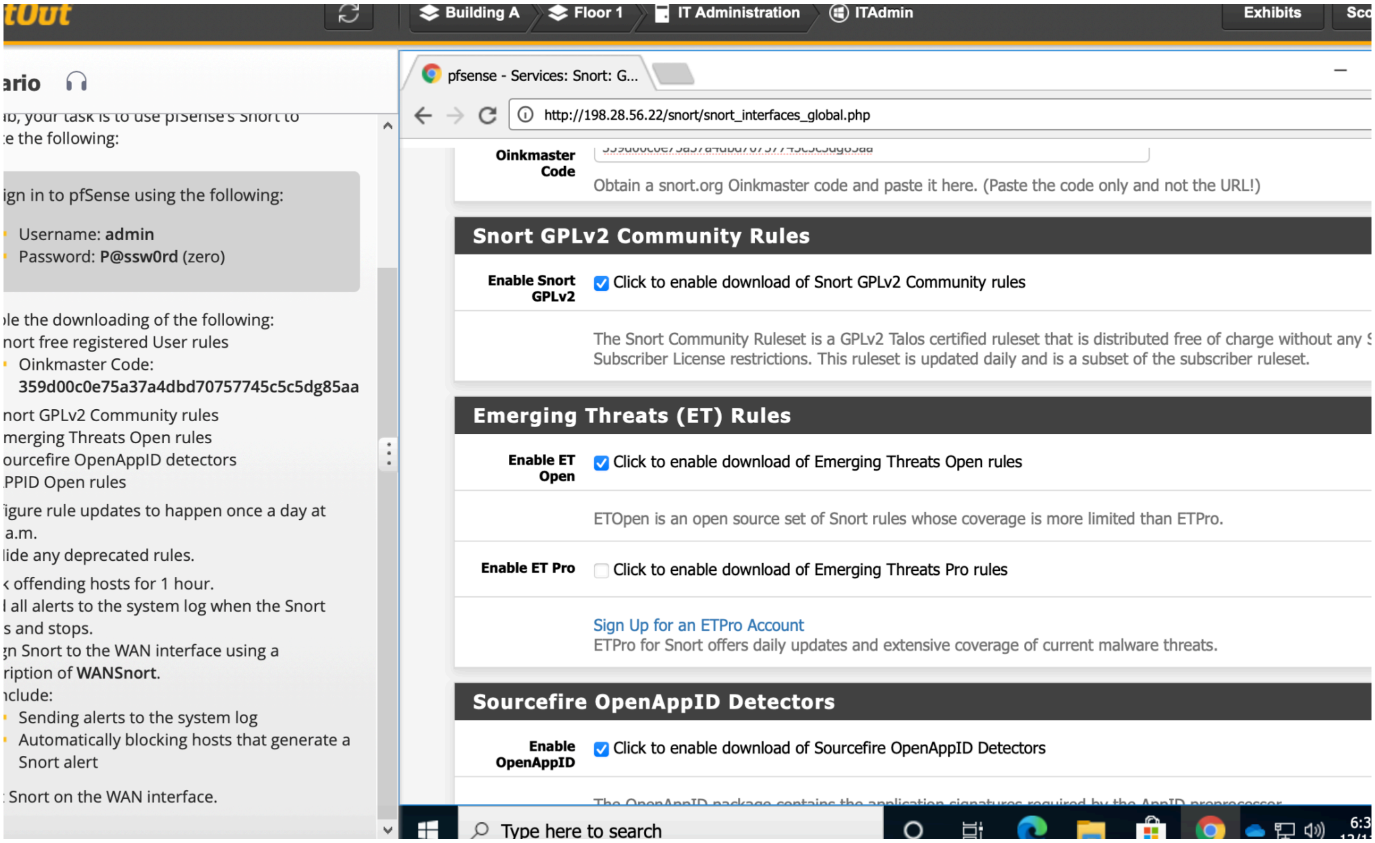
Enable Snort GPLv2 □ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any S Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

I will also add the Oinkmaster code provided to us by the lab as shown.

Robert Carpenter
github.com/robertmcarpenter
Wed December 11th 2024


tOut
Building A
Floor 1
IT Administration
ITAdmin
Exhibits
Sco
ario
pfsense - Services: Snort: G...
http://198.28.56.22/snort/snort_interfaces_global.php
Type here to search
6:3

ıb, your task is to use pfSense's Snort to
:e the following:

ign in to pfSense using the following:

- Username: **admin**
- Password: **P@ssw0rd** (zero)

ɔle the downloading of the following:
nort free registered User rules
- Oinkmaster Code: **359d00c0e75a37a4dbd70757745c5c5dg85aa**

nort GPLv2 Community rules
merging Threats Open rules
ourcefire OpenAppID detectors
PPID Open rules

igure rule updates to happen once a day at
a.m.
lide any deprecated rules.

‹ offending hosts for 1 hour.
l all alerts to the system log when the Snort
s and stops.
ʒn Snort to the WAN interface using a
ription of **WANSnort**.
ıclude:
- Sending alerts to the system log
- Automatically blocking hosts that generate a Snort alert

: Snort on the WAN interface.

Oinkmaster Code
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

Enable Snort GPLv2 ☑ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any S
Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

Enable ET Open ☑ Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

Enable ET Pro □ Click to enable download of Emerging Threats Pro rules

Sign Up for an ETPro Account
ETPro for Snort offers daily updates and extensive coverage of current malware threats.

Sourcefire OpenAppID Detectors

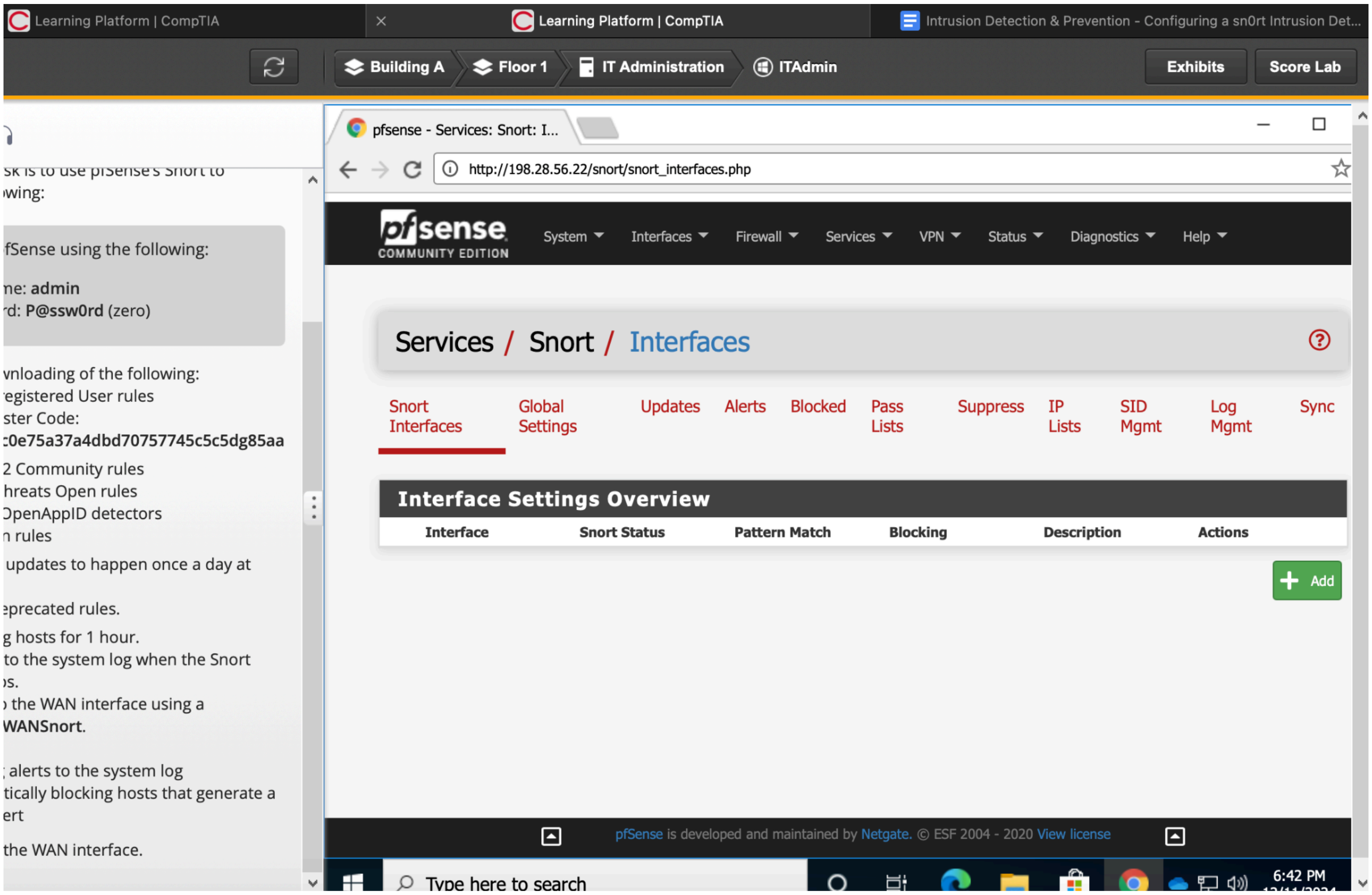
Enable OpenAppID ☑ Click to enable download of Sourcefire OpenAppID Detectors

The OpenAppID package contains the application signatures required by the AppID preprocessor

After we've set our configuration on this page, we need to point snort to an interface to "listen" to packets in order to determine their legitimacy.

To do that I'll navigate to **Services > Snort Interface**

Robert Carpenter
github.com/robertmcarpenter
Wed December 11th 2024



sk is to use pfSense's Snort to
wing:

fSense using the following:

ne: **admin**
rd: **P@ssw0rd** (zero)

vnloading of the following:
egistered User rules
ster Code:
:0e75a37a4dbd70757745c5c5dg85aa
2 Community rules
hreats Open rules
OpenAppID detectors
n rules
updates to happen once a day at

eprecated rules.
g hosts for 1 hour.
to the system log when the Snort
ns.
the WAN interface using a
WANSnort.

; alerts to the system log
tically blocking hosts that generate a
ert

the WAN interface.

http://198.28.56.22/snort/snort_interfaces.php

Services / Snort / Interfaces

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking	Description	Actions

pfSense is developed and maintained by Netgate. © ESF 2004 - 2020 View license

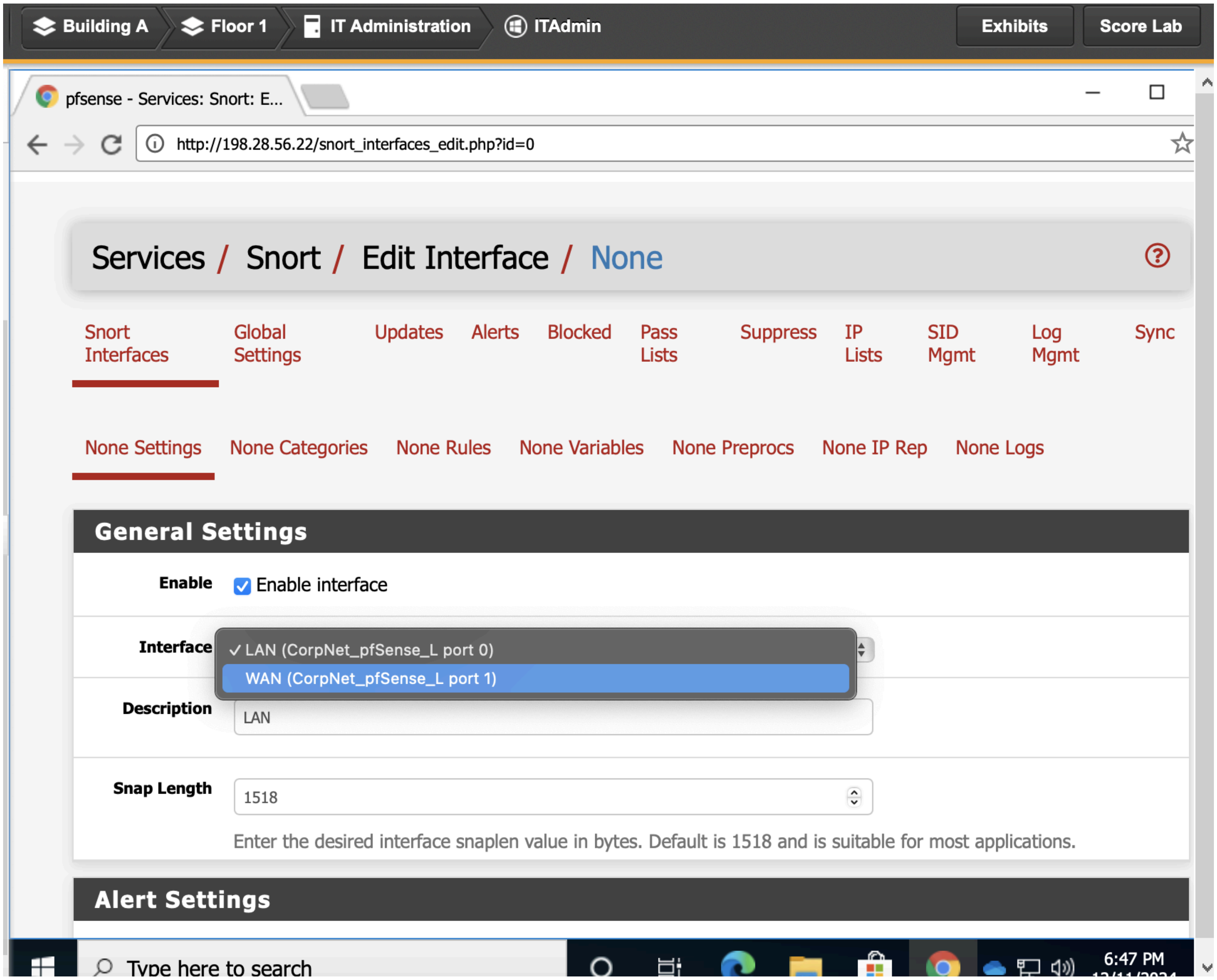
I'll hit the Green Add button to assign Snort to my WAN interface.

We need to do the following:

Assign Snort to the WAN interface using a description of **WANSnort**.

- Include:
  - Sending alerts to the system log
  - Automatically blocking hosts that generate a Snort alert
- Start Snort on the WAN interface.

Robert Carpenter
github.com/robertmcarpenter
Wed December 11th 2024


Building A
Floor 1
IT Administration
ITAdmin
Exhibits
Score Lab
pfsense - Services: Snort: E...
http://198.28.56.22/snort_interfaces_edit.php?id=0

Services / Snort / Edit Interface / None

General Settings

Enable ☑ Enable interface

Interface ✓ LAN (CorpNet_pfSense_L port 0)
WAN (CorpNet_pfSense_L port 1)

Description LAN

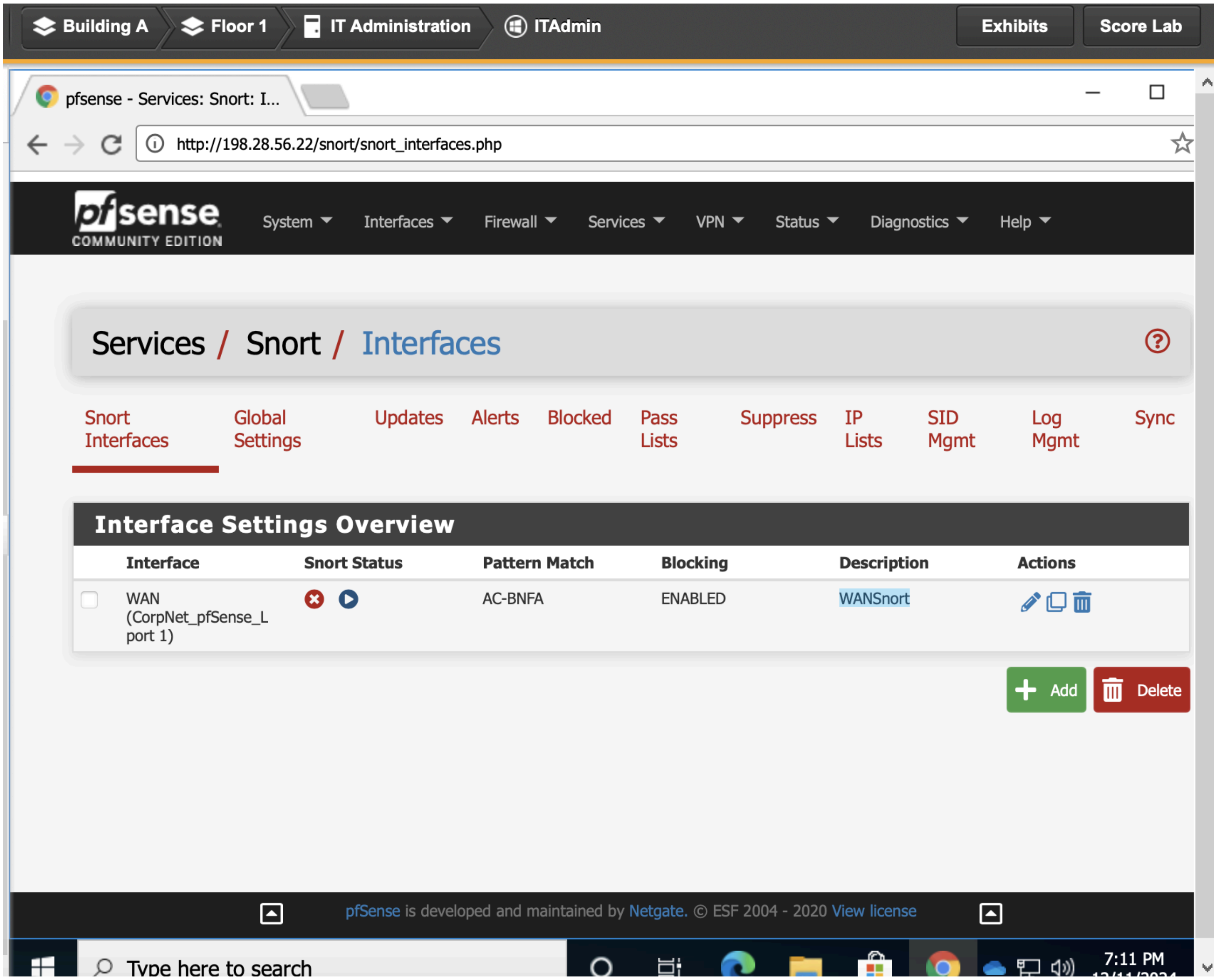
Snap Length 1518

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

Alert Settings

Now that we’ve added the configuration for this WAN interface , the Snort menu will populate with the config we just added.

Robert Carpenter
github.com/robertmcarpenter
Wed December 11th 2024



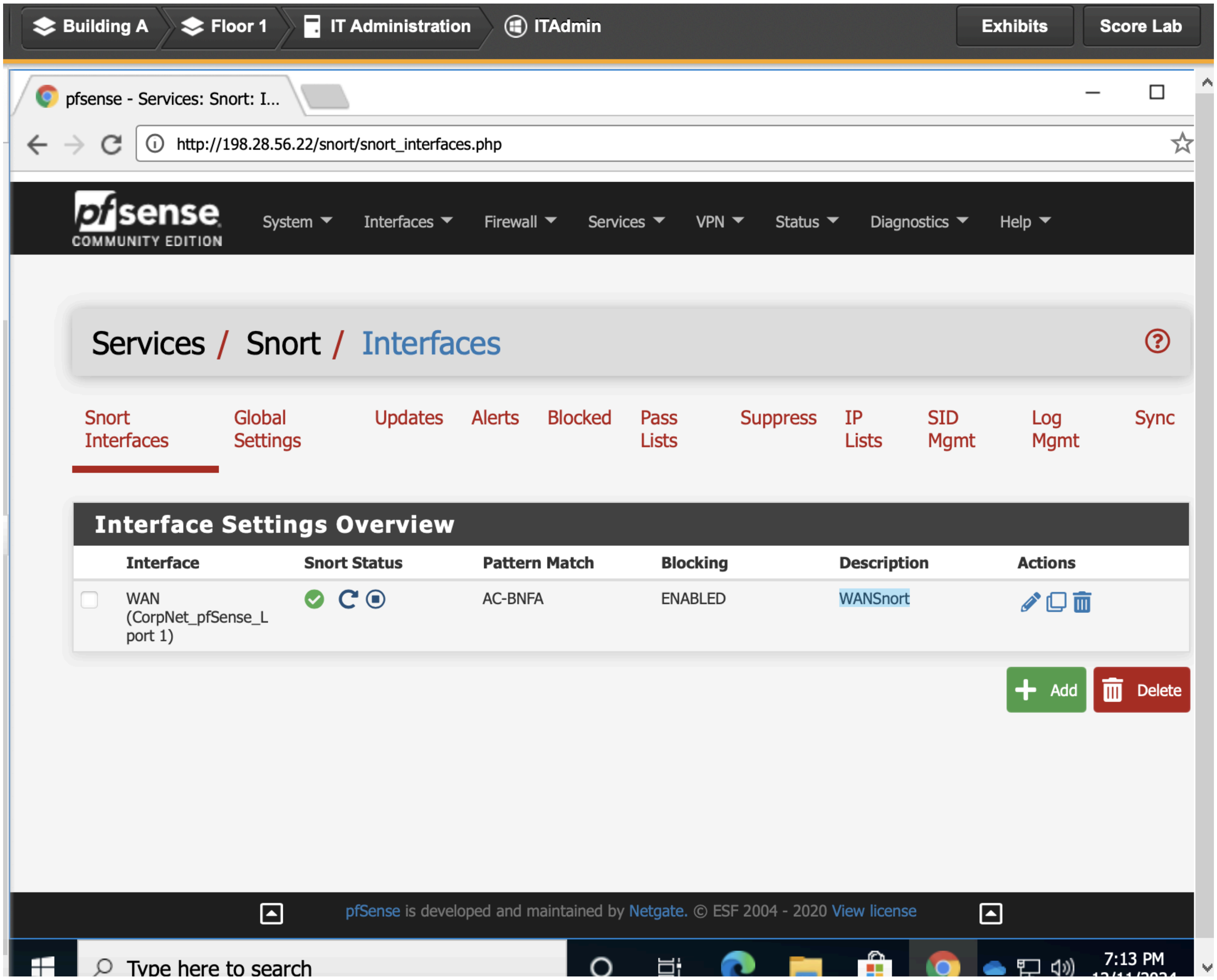
Services / Snort / Interfaces

Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking	Description	Actions
□	WAN (CorpNet_pfSense_L port 1)	☒ ▶	AC-BNFA	ENABLED	WANSnort	

The last task of this lab is to manually start the Snort service. I can do that by clicking the PLay button on the **Snort Status. After I click the button I see the following;**

Robert Carpenter
github.com/robertmcarpenter
Wed December 11th 2024



Services / Snort / Interfaces

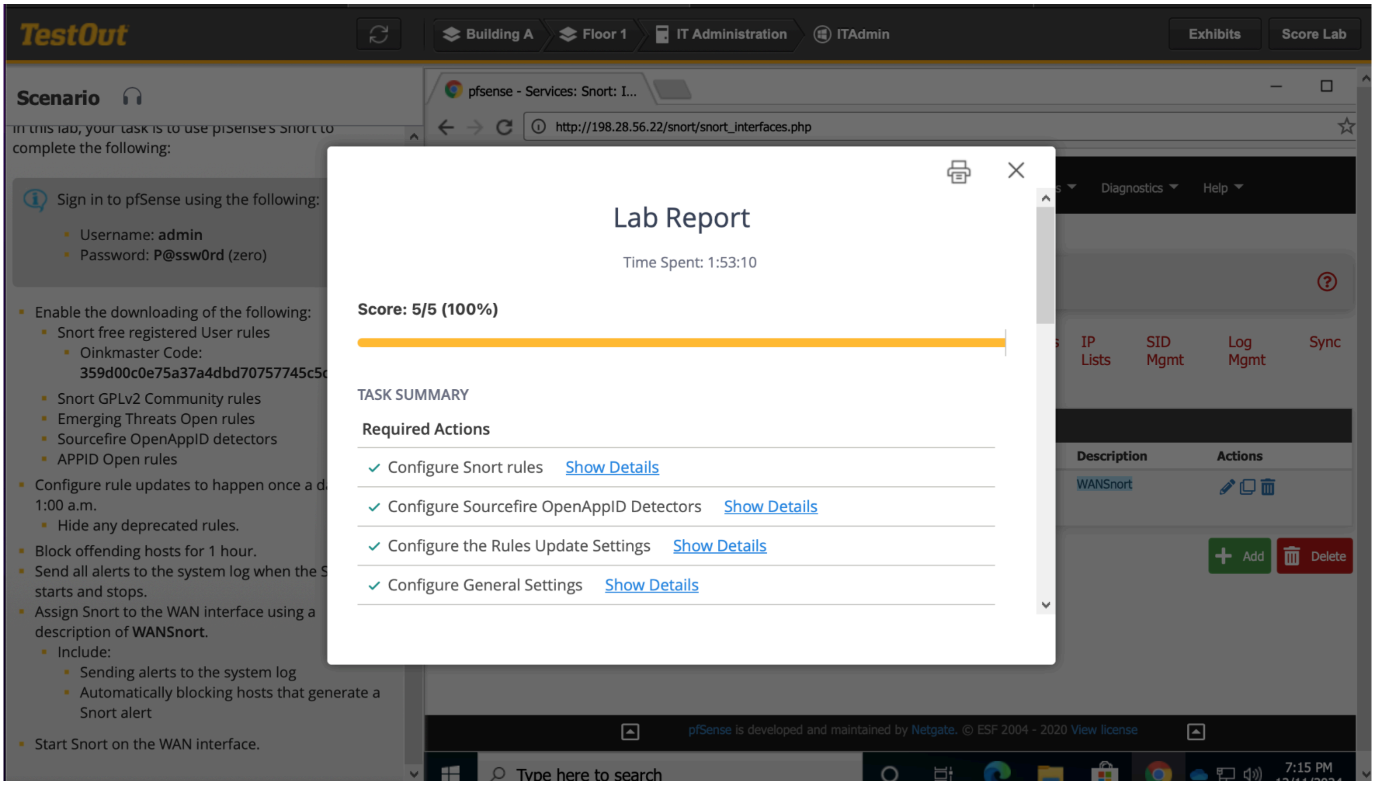
Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking	Description	Actions
□	WAN (CorpNet_pfSense_L port 1)	✓	AC-BNFA	ENABLED	WANSnort	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2020 View license

This now concludes the lab! We've completed all the task and the configurations we set are now active and running on the Snort service within our pfSense Security Environment!

Robert Carpenter
github.com/robertmcarpenter
Wed December 11th 2024



Scenario

In this lab, your task is to use pfSense's Snort to complete the following:

Sign in to pfSense using the following:

- Username: **admin**
- Password: **P@ssw0rd** (zero)

- Enable the downloading of the following:
  - Snort free registered User rules
    - Oinkmaster Code: **359d00c0e75a37a4dbd70757745c5c**
  - Snort GPLv2 Community rules
  - Emerging Threats Open rules
  - Sourcefire OpenAppID detectors
  - APPID Open rules
- Configure rule updates to happen once a d 1:00 a.m.
  - Hide any deprecated rules.
- Block offending hosts for 1 hour.
- Send all alerts to the system log when the S starts and stops.
- Assign Snort to the WAN interface using a description of **WANSnort**.
  - Include:
    - Sending alerts to the system log
    - Automatically blocking hosts that generate a Snort alert
- Start Snort on the WAN interface.

Description	Actions
WANSnort	

Lab Report

Time Spent: 1:53:10

Score: 5/5 (100%)

TASK SUMMARY

Required Actions

- ✓ Configure Snort rules Show Details
- ✓ Configure Sourcefire OpenAppID Detectors Show Details
- ✓ Configure the Rules Update Settings Show Details
- ✓ Configure General Settings Show Details

pfSense is developed and maintained by Netgate. © ESF 2004 - 2020 View license