

Implementation Report: C2 Simulation Exercise

Table Of Contents

▼ Proxmox

- Preparing for Installation
- Installation Process
- Initial Configuration

▼ Splunk

- Installation guide
- Starting Splunk
- Accessing Splunk

▼ Guide to Setting up pfSense and Suricata in Splunk

- Step 1: pfSense SSH Setup
- Step 2: pfSense Suricata Install
- Step 3: Splunk Setup
 - Splunk Index Setup
 - Splunk Apps Installation
 - Splunk Data Inputs
- Step 4: pfSense Remote Logging Setup
- Step 5: Configuring pfSense Suricata
- Step 6: pfSense Splunk Forwarder and Shipping of Suricata logs

▪ Create Alerts

▪ Download abuse.ch feeds

▼ Dashboard Creation

- Add Report Correlating threatfox ports to suricata logs

▼ Caldera

- Installation on kali

▼ Agents

- 1. Access the CALDERA Web Interface
- 2. Navigate to the Agents Tab
- 3. Select and Install Agents
- 4. Deploy the Agent
- 5. Verify Agent Installation
- 6. Manage and Configure Agents
- 7. Use Agents in Operations

▼ PfSense

▪ Installation

▼ Configuration

- 1. Prepare VirtualBox Networks
- 2. Create pfSense Virtual Machine
- 3. Install pfSense
- 4. Initial Setup and Interface Assignment
- 5. Access pfSense Web Interface
- 6. WebConfigurator Setup Wizard

- 7. Configure OPT1 Interface

- 8. Firewall Rules

- 9. Testing the Setup

- 10. Final Adjustments

▼ Suricata

- ▼ Installation on pfSense

- Forward suricata logs to splunk with cron and rsync

- Configuring Suricata on pfSense

▼ Detecting encrypted beacons

- ▼ Caldera

- SSL

- Deploy https agents

- ▼ Zeek

- Enable ja3 fingerprinting

- Splunk Setup

Proxmox

Proxmox VE (Virtual Environment) is an open-source server virtualization platform. It is designed for managing Virtual Machines (VMs), containers, and associated storage, all through a single web-based interface. It integrates KVM (Kernel-based Virtual Machine) for full virtualization and LXC (Linux Containers) for containerization.

Preparing for Installation

1. Download Proxmox VE ISO
 - Go to the [Proxmox VE download page](#).
 - Download the latest Proxmox VE ISO image.
2. Create a Bootable USB Drive
 - Use a tool like Rufus (Windows) or Balena Etcher (Linux/Mac) to create a bootable USB drive.
 - Select the downloaded Proxmox VE ISO and follow the tool's instructions to create the bootable media.

Installation Process

1. Boot from USB
 - Insert the bootable USB drive into the server.
 - Power on the server and access the BIOS/UEFI settings to set the USB drive as the primary boot device.
 - Save the settings and reboot.
2. Start the Installation
 - When the Proxmox VE installer menu appears, select Install Proxmox VE.
 - Read and accept the EULA (End User License Agreement).
3. Configure Disk and System
 - Disk Selection: Choose the hard disk where Proxmox VE will be installed. All data on this disk will be erased.
 - Country, Time Zone, and Keyboard Layout:
 - Set your location, time zone, and preferred keyboard layout.
 - Administrator Password:
 - Set a strong password for the `root` user.
 - Enter a valid email address for system notifications.
4. Network Configuration
 - Hostname: Set a unique hostname for the Proxmox server.
 - IP Address: Assign a static IP address, subnet mask, and gateway.
 - DNS Server: Set the DNS server address.
 - Configure the network settings
5. Finalize Installation
 - Review your settings and click Install.
 - The installation will proceed, and the server will reboot when completed.

Initial Configuration

1. Access the Web Interface
 - After the reboot, remove the USB drive.
 - Open a web browser on a device connected to the same network and navigate to: https://<Proxmox_IP>:8006
 - Log in using the `root` username and the password set during installation.
2. Update Proxmox VE
 - Navigate to Datacenter -> Updates.
 - Click Refresh to fetch the latest updates.
 - Install any available updates.
3. Configure Storage and Network (Optional)
 - Storage: Set up additional storage under Datacenter -> Storage.
 - Network: Manage network interfaces, bridges, and VLANs under Datacenter -> Network

Splunk

Splunk is a powerful data platform used for searching, analyzing, and visualizing machine-generated data. It helps organizations gain valuable insights from their data to improve operations, security, and business decisions.

Installation guide

Installing Splunk on Debian

- Download the Splunk .deb file from the Splunk website.
- Use the following command to install it:

```
sudo dpkg -i splunk-<version>-linux-<architecture>.deb
```

Starting Splunk

```
sudo /opt/splunk/bin/splunk start
```

Accessing Splunk

Open a web browser and navigate to `http://<VMIP>:8000` to complete the initial setup.

Guide to Setting up pfSense and Suricata in Splunk

Step 1: pfSense SSH Setup

The first thing you'll need to do is log into your pfSense web GUI and go to **System > Advanced** to enable secure shell access to your router if you have not done so. This will be needed for future steps.

The best practice here would be to set up access with a public key and password but for the sake of demonstration, we're simply going to enable password authentication at this time.

The screenshot shows the pfSense WAN Rules configuration page. At the top, there are tabs for WAN Settings, WAN Categories, WAN Rules, WAN Flow/Stream, WAN App Parsers, WAN Variables, WAN Barnyard2, and WAN IP Rep. The WAN Rules tab is selected.

Automatic flowbit resolution

Resolve Flowbits: Auto-enable rules required for checked flowbits. Default is Checked. Suricata will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

View rules: [View](#). Click to view auto-enabled rules required to satisfy flowbit dependencies.

Note: Auto-enabled rules generating unwanted alerts should have their GID:SID added to the Suppression List for the interface.

Snort IPS Policy selection

Use IPS Policy: Use rules from one of three pre-defined Snort IPS policies. **Note:** You must be using the Snort rules to use this option. Selecting this option disables manual selection of Snort rules categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort rules set.

IPS Policy Selection: Connectivity. Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as Flash in an Excel file. Maximum Detection encompasses vulnerabilities from 2005 or later with a CVSS score of at least 7.5 along with critical malware and exploit kit rules. The Maximum Detection policy favors detection over rated throughput. In some situations this policy can and will cause significant throughput reductions.

IPS Policy Mode: Policy. When Policy is selected, this will automatically change the action for rules in the selected IPS Policy from their default action of alert to the action specified in the policy metadata (typically drop, but may be alert for some policy rules).

Select the rulesets (Categories) Suricata will load at startup

Green circle: - Category is auto-enabled by SID Mgmt conf files
Red circle: - Category is auto-disabled by SID Mgmt conf files

Enabled **Ruleset: Snort GPLv2 Community Rules**

Snort GPLv2 Community Rules (Talos-certified)

Enabled **Ruleset: ET Open Rules** **Snort Rules have not been downloaded.**

emerging-activex.rules
 emerging-adware_pup.rules
 emerging-attack_response.rules
 emerging-botcc.portgrouped.rules
 emerging-botcc.rules
 emerging-chat.rules
 emerging-clamdy.rules
 emerging-coinminer.rules
 emerging-compromised.rules
 emerging-current_events.rules
 emerging-deleted.rules
 emerging-dns.rules
 emerging-dos.rules

Select All **Unselect All** **Save**

Once you have enabled SSH in the web GUI, verify that you can ssh to the router by using PuTTY, PowerShell, or your favorite terminal environment. `ssh root@ip-of-router`. The password would be the same password you use to authenticate to the web GUI.

Alert and Block Settings

Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Suricata alert.
IPS Mode	Legacy Mode
Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata 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 Suricata 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! If the hardware NIC driver does not support Netmap, using Inline Mode can result in a firewall system crash! If problems are experienced with Inline Mode, switch to Legacy Mode instead.	
Kill States	<input checked="" type="checkbox"/> Checking this option will kill firewall states for the blocked IP. Default is Checked.
Which IP to Block	SRC
Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value.	
Block On DROP Only	<input type="checkbox"/> Checking this option will insert blocks only when rule signatures having the DROP action are triggered. When not checked, any rule action (ALERT or DROP) will generate a block of the offending host. Default is Not Checked.

Step 2: pfSense Suricata Install

To install Suricata, it's as simple as clicking a few buttons. We will need to go to **System -> Package Manager -> Available Packages**. Scroll down until you find "Suricata" and then click install.

Step 3: Splunk Setup

Splunk Index Setup

Before we get any further, we need to configure Splunk to receive our data.

To make things simple, we are going to create two indexes. One for pfSense called "network," and another for Suricata called "ids." I recommend you create and keep a table of indexes handy so you know where to look for your data within Splunk. This will solve future headaches when you're looking for certain events.

1. To create an index, log into Splunk and then click **Settings -> Indexes**.

```
Alderaan:Downloads aoneil$ ls
└─+COMPACT_MANIFEST └─+MANIFEST  └─opt  └─splunkforwarder-8.0.3-a6754d8441bf-freebsd-11.1-amd64.txz
Alderaan:Downloads aoneil$ scp -r opt/ root@10.10.10.1:/root/
Password for root@pfSense.home:†
```

2. Once on the "Indexes" page, we will want to click "New Index" in the top right corner of the page. You will then be presented with options for creating a new index.
3. For the first index, we will name it "network." You can leave the rest of the settings alone unless you want to set up index retention which can be learned about [here](#).
4. Once finished, go ahead and save the index.

Repeat this process for the other index needed called "ids".

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for 'Austin O'Neil', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar. Below the navigation is a secondary menu with 'Search', 'Anal...', 'Search & Reporting' (which is highlighted with a blue border), 'Enterprise Security', and 'Docker Simple'. To the right of this menu is a 'Dashboards' section. Further down, there's a search bar with 'Last 24 hours' and a green search button, along with a 'Fast Mode' toggle. On the left, under 'Search', there's a 'How to Search' section with links to 'Documentation' and 'Tutorial', and a 'What to Search' section showing statistics: '102,659 Events INDEXED', '2 years ago EARLIEST EVENT', and 'a month ago LATEST EVENT'. A 'Data Summary' button is also present. At the bottom left, there's a link to 'Search History' and a URL in the address bar: 'https://10.20.0.3:8000/en-US/manager/search/apps/local'.

Splunk Apps Installation

Next, we need to download a few of the Splunk apps from splunkbase.splunk.com

The following links will take you to the apps we will be using in this tutorial:

- [Splunk Common Information Model \(CIM\)](#) – “The CIM helps you to normalize your data to match a common standard, using the same field names and event tags for equivalent events from different sources or vendors.” This will allow us to build alerts and reports easily after everything is set up.
- [TA-pfSense](#) – This allows Splunk to extract fields from pfSense logs.
- [Splunk TA for Suricata](#) – This allows Splunk to extract fields from Suricata logs.

Go ahead and download those apps. You'll need to install them onto your Splunk server and on your pfSense Splunk forwarder, which we'll set up later in the tutorial.

To install the apps on your Splunk server, click **Apps > Manage Apps** in the top left corner.

```
Alderaan:Downloads aoneil$ ls
splunkforwarder-8.0.3-a6754d8441bf-freebsd-11.1-amd64.txz
Alderaan:Downloads aoneil$ tar xvzf splunkforwarder-8.0.3-a6754d8441bf-freebsd-11.1-amd64.txz|
```

We will then want to click “Install app from file” and choose one of the apps you recently downloaded. Once chosen, click “Upload” and repeat until all three

apps are uploaded.

Remote Logging Options			
Enable Remote Logging	<input checked="" type="checkbox"/> Send log messages to remote syslog server		
Source Address	Default (any)		
This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.			
NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.			
IP Protocol	IPv4		
This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; if an IP address of the selected type is not found on the chosen interface, the other type will be tried.			
Remote log servers	10.20.0.3:5147	IP[:port]	IP[:port]
Remote Syslog Contents	<input checked="" type="checkbox"/> Everything <input type="checkbox"/> System Events <input type="checkbox"/> Firewall Events <input type="checkbox"/> DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns) <input type="checkbox"/> DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client) <input type="checkbox"/> PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client) <input type="checkbox"/> Captive Portal Events <input type="checkbox"/> VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server) <input type="checkbox"/> Gateway Monitor Events <input type="checkbox"/> Routing Daemon Events (RADVD, LPRng, RIP, OSPF, BGP)		

We won't need to configure any of the installed apps. Once all of the apps are uploaded, we can continue to the next step.

Splunk Data Inputs

Now that we have the apps installed, we need to configure UDP receiving ports. This can be achieved by going to **Settings -> Data Inputs**. Click "+ Add New" next to UDP. We need to configure a UDP port to receive pfSense logs from the GUI.

We will be taken to the add data page within Splunk. Let's go ahead and add in a port to receive our logs. I am going to use port 5147.

WAN Settings		WAN Categories	WAN Rules	WAN Flow/Stream	WAN App Parsers	WAN Variables	WAN Barnyard2	WAN IP Rep
General Settings								
Enable	<input checked="" type="checkbox"/> Checking this box enables Suricata inspection on the interface.							
Interface	<input type="button" value="WAN"/> Choose which interface this Suricata instance applies to. In most cases, you will want to use WAN here if this is the first Suricata-configured interface.							
Description	<input type="button" value="WAN"/> Enter a meaningful description here for your reference. The default is the interface name.							
Logging Settings								
Send Alerts to System Log	<input type="checkbox"/> Suricata will send Alerts from this interface to the firewall's system log.							
Enable Stats Log	<input type="checkbox"/> Suricata will periodically log statistics for the interface. Default is Not Checked.							
Enable HTTP Log	<input checked="" type="checkbox"/> Suricata will log decoded HTTP traffic for the interface. Default is Checked.							
Append HTTP Log	<input checked="" type="checkbox"/> Suricata will append-to instead of clearing HTTP log file when restarting. Default is Checked.							
Log Extended HTTP Info	<input checked="" type="checkbox"/> Suricata will log extended HTTP information. Default is Checked.							
Enable TLS Log	<input checked="" type="checkbox"/> Suricata will log TLS handshake traffic for the interface. Default is Not Checked.							
Enable TLS Store	<input checked="" type="checkbox"/> Suricata will log and store TLS certificates for the interface. Default is Not Checked.							
Log Extended TLS Info	<input checked="" type="checkbox"/> Suricata will log extended TLS info such as fingerprint. Default is Checked.							
Enable Tracked-Files Log	<input checked="" type="checkbox"/> Suricata will log tracked files in JavaScript Object Notation (JSON) format. Default is Not Checked.							
Append Tracked-Files Log	<input checked="" type="checkbox"/> Suricata will append-to instead of clearing Tracked Files log file when restarting. Default is Checked.							
Enable Logging Magic for Tracked-Files	<input checked="" type="checkbox"/> Suricata will force logging magic on all logged Tracked Files. Default is Not Checked.							
Tracked-Files Checksum	<input type="button" value="MD5"/> Suricata will generate checksums for all logged Tracked Files using the chosen algorithm. Default is None.							
Enable File-Store	<input type="checkbox"/> Suricata will extract and store files from application layer streams. Default is Not Checked. Warning: This will consume a significant amount of disk space on a busy network when enabled.							
Enable Packet Log	<input type="checkbox"/> Suricata will log decoded packets for the interface in pcap-format. Default is Not Checked. This can consume a significant amount of disk space when enabled.							
EVE Output Settings								
EVE JSON Log	<input checked="" type="checkbox"/> Suricata will output selected info in JSON format to a single file or to syslog. Default is Not Checked.							
EVE Output Type	<input type="button" value="FILE"/> Select EVE log output destination. Choosing FILE is suggested, and is the default value.							

In the source type drop-down, type "pfSense". We need to select pfSense without the ":" as seen in the image below.

The screenshot shows the "General Logging Options" section of the pfSense Settings. It includes:

- Forward/Reverse Display:** A checkbox labeled "Show log entries in reverse order (newest entries on top)" is checked.
- GUI Log Entries:** A text input field set to "50". Below it is a note: "This is only the number of log entries displayed in the GUI. It does not affect how many entries are contained in the actual log files."
- Log file size (Bytes):** A dropdown menu set to "Bytes". Below it is a note: "Logs are held in constant-size circular log files. This field controls how large each log file is, and thus how many entries may exist inside the log. By default this is approximately 500KB per log file, and there are nearly 20 such log files." A note below states: "NOTE: Log sizes are changed the next time a log file is cleared or deleted. To immediately increase the size of the log files, first save the options to set the size, then clear all logs using the "Reset Log Files" option farther down this page. Be aware that increasing this value increases every log file size, so disk usage will increase significantly."
- Disk space currently used by log files:** "2.9G Remaining disk space for log files: 96G"
- Log firewall default:** A checkbox labeled "Log packets matched from the default block rules in the ruleset" is checked.

The next setting we need to change is the host field. Select “Custom” and type in the hostname of your pfSense router. Once that’s complete, select the index drop-down and select the “network” index we created earlier.

The screenshot shows the "Input Settings" step of the Splunk "Add Data" wizard. The steps are: "Select Source" (done), "Input Settings" (in progress), "Review", and "Done".

Input Settings: Optionally set additional input parameters for this data input as follows:

Source type: A dropdown menu is open, showing suggestions: "pfSense", "pfSense:dhcpd", "pfSense:filterlog", "pfSense:nginx", "pfSense:openvpn", and "pfSense:unbound". The suggestion "pfSense" is highlighted. Below the dropdown is a button "Select Source Type ▾".

App context: A dropdown menu is open, showing "App Context" and "Search & Reporting (search) ▾".

The URL in the browser address bar is: <https://10.20.0.3:8000/en-US/manager/search/adddatamethods/inputsettings#>

Continue to the next page by clicking “Review,” verify your new data input settings, and click “Submit.”

Once that is complete, we need to set up our receiving port for our forwarder. Go to Settings -> Forwarding and Receiving. Click “Add New” next to “Configure receiving.” In the “Listen on this port” field, enter “9997.” Once that is done, hit “Save” and then we can go back to the Splunk homepage by clicking on “Splunk->” in the top left corner.

Step 4: pfSense Remote Logging Setup

We need to set up pfSense to log to the new index and data input we just set up. To do so, in pfSense's web GUI go to the NAVbar and select **Status -> System Logs**. Once there, we need to go to the settings tab and scroll down to the bottom of the page.

EVE Output Settings	
EVE JSON Log	<input checked="" type="checkbox"/> Suricata will output selected info in JSON format to a single file or to syslog. Default is Not Checked.
EVE Output Type	FILE
Select EVE log output destination. Choosing FILE is suggested and is the default value. "Redis" is used for output to a Redis server, and the UNIX Socket options output to a user-created socket.	
EVE HTTP XFF Support	<input type="checkbox"/> Log X-Forwarded-For IP addresses. Default is Not Checked.
EVE Ethernet MAC	<input type="checkbox"/> Log Ethernet header in events when available. Default is Not Checked.
EVE Log Alerts	<input checked="" type="checkbox"/> Suricata will output Alerts via EVE
EVE Log Alert Payload Data Formats	BOTH
Log the payload data with alerts. Options are No (disable payload logging), Only Printable (lossy) format, Only Base64 encoded or Both. See Suricata documentation.	
EVE Log Alert details	<input checked="" type="checkbox"/> Log a packet dump with alerts. <input checked="" type="checkbox"/> Log additional HTTP data. <input checked="" type="checkbox"/> Include App Layer metadata. <input type="checkbox"/> Log final action taken on packet by the engine <input type="checkbox"/> Log packets for rules using the "tag" keyword
EVE Log Drops	<input checked="" type="checkbox"/> Suricata will output Drops via EVE
EVE Log Drops Options	<input checked="" type="checkbox"/> Log alerts that caused drops. Default is "Checked". <input type="checkbox"/> Log final action taken on packet by the engine All
"Start" logs only a single drop per flow direction. "All" logs each dropped pkt.	

Go ahead and check the "Enable Remote Logging" box. Enter the IP address of your Splunk server followed by the port number we set up in the Data Inputs section. The last thing we need to do is check the "Everything" box under Remote Syslog Contents. Save the page.

The screenshot shows the Splunk Add Data interface. At the top, there's a navigation bar with 'splunk>enterprise' and various links like 'Apps', 'Austin O'Neil', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the navigation is a progress bar with four steps: 'Select Source' (green dot), 'Input Settings' (green dot), 'Review' (white circle), and 'Done' (white circle). A 'Review' button is also present. The main content area has two sections: 'Host' and 'Index'. The 'Host' section contains text about host values and configuration options, with a 'Method?' dropdown showing 'IP', 'DNS', and 'Custom', and a 'Host field value' input field containing 'pfSense.home'. The 'Index' section contains text about index selection and troubleshooting, with an 'Index' dropdown set to 'network' and a 'Create a new index' link.

At this point, we should be able to go back to our Splunk instance and run the following search.

```
index=network sourcetype=pfSense*
```

You should now see pfSense events returning from your Splunk search with all fields from the TA extracted! If you don't see all fields being extracted, be sure to run the search in "Verbose Mode."

Please Choose The Type Of Rules You Wish To Download		
Install ETOpen Emerging Threats rules	<input checked="" type="checkbox"/> ETOpen is a free open source set of Suricata rules whose coverage is more limited than ETPro.	<input type="checkbox"/> Use a custom URL for ETOpen downloads
Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETOpen rules.		
Install ETPro Emerging Threats rules	<input type="checkbox"/> ETPro for Suricata offers daily updates and extensive coverage of current malware threats.	<input type="checkbox"/> Use a custom URL for ETPro rule downloads
The ETPro rules contain all of the ETOpen rules, so the ETOpen rules are not required and are disabled when the ETPro rules are selected. Sign Up for an ETPro Account . Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETPro rules.		
ETPro Subscription Configuration Code	<input type="text"/>	
Obtain an ETPro subscription code and paste it here.		
Install Snort rules	<input checked="" type="checkbox"/> Snort free Registered User or paid Subscriber rules	<input type="checkbox"/> Use a custom URL for Snort rule downloads
Sign Up for a free Registered User Rules Account Sign Up for paid Snort Subscriber Rule Set (by Talos)		
Enabling the custom URL option will force the use of a custom user-supplied URL when downloading Snort Subscriber rules.		
Snort Rules Filename	<input type="text" value="community-rules.tar.gz"/>	
Enter the rules tarball filename (filename only, do not include the URL.) Example: snortrules-snapshot-29151.tar.gz DO NOT specify a Snort3 rules file! Snort3 rules are incompatible with Suricata and will break your installation!		
Snort Oinkmaster Code	<input type="text" value="OINK CODE HERE"/>	
Obtain a snort.org Oinkmaster code and paste it here.		
Install Snort GPLv2 Community rules	<input checked="" type="checkbox"/> The Snort Community Ruleset is a GPLv2 Talos-certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions.	<input type="checkbox"/> Use a custom URL for Snort GPLv2 rule downloads
This ruleset is updated daily and is a subset of the subscriber ruleset. If you are a Snort Subscriber Rules customer (paid subscriber), the community ruleset is already built into your download of the Snort Subscriber rules, and there is no benefit in adding this rule set separately.		
Hide Deprecated Rules Categories	<input checked="" type="checkbox"/> Hide deprecated rules categories in the GUI and remove them from the configuration. Default is Not Checked.	
Rules Update Settings		
Update Interval	<input type="text" value="12 HOURS"/>	
Please select the interval for rule updates. Choosing NEVER disables auto-updates.		
Hint: In most cases, every 12 hours is a good choice.		
Update Start Time	<input type="text" value="00:30"/>	
Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.		
Live Rule Swap on Update	<input checked="" type="checkbox"/> Enable "Live Swap" reload of rules after downloading an update. Default is Not Checked	
When enabled, Suricata will perform a live load of the new rules following an update instead of a hard restart. If issues are encountered with live load, uncheck this option to perform a hard restart of all Suricata instances following an update.		
GeoLite2 DB Update	<input checked="" type="checkbox"/> Enable downloading of free GeoLite2 Country IP Database updates. Default is Not Checked	

Step 5: Configuring pfSense Suricata

Okay, we have pfSense logs inside Splunk. Now we need to get our IDS setup and then get the logs shipped to Splunk. Let's get started! Since we installed Suricata in a past step, we just need to configure it.

Let's go to **Services -> Suricata** inside of pfSense. We first need to go to the Global Settings tab and enable rules to download. Since free is good enough for my environment, I enabled ETOpen Emerging Threats and I set up a Snort account to download the free community Snort rules. [You can sign up for an account here](#).

You can change the update interval to automatically download the new rules added to ETOpen and Snort Community rule base.

Automatic flowbit resolution

Resolve Flowbits Auto-enable rules required for checked flowbits

Default is Checked. Suricata will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

View rules



Click to view auto-enabled rules required to satisfy flowbit dependencies

Note: Auto-enabled rules generating unwanted alerts should have their GID:SID added to the Suppression List for the interface.

Snort IPS Policy selection

Use IPS Policy Use rules from one of three pre-defined Snort IPS policies

Note: You must be using the Snort rules to use this option.

Selecting this option disables manual selection of Snort rules categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort rules set.

IPS Policy Selection



Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as Flash in an Excel file. Maximum Detection encompasses vulnerabilities from 2005 or later with a CVSS score of at least 7.5 along with critical malware and exploit kit rules. The Maximum Detection policy favors detection over rated throughput. In some situations this policy can and will cause significant throughput reductions.

Next, we want to go to the “Updates” tab and hit “Force” to force download all the rules we selected on the previous page.

Once that is done, we can return to the Interfaces tab and click the “+ Add” button to set up the WAN interface. There will be a few screenshots below—these are what I determined to give the best logging output. We need Suricata to log in EVE JSON mode.

The screenshot shows the Splunk Enterprise interface with the "Indexes" dashboard. On the left, there is a table listing four indexes: "_audit", "_internal", "_introspection", and "_metrics". Each row has "Actions" (Edit, Delete, Disable), "Type" (Events or Metrics), "App" (system), and "Current Size". The "_audit" index is currently selected. A context menu is open over the "_audit" row, with "Edit" highlighted. Other options in the menu are "Delete" and "Disable". The menu is organized into sections: Monitoring Console, KNOWLEDGE, DATA, SYSTEM, and USERS AND AUTHENTICATION. The "Edit" option is located under the "Monitoring Console" section.

We now have to determine if we want to block offenders or not. You have the option to pick between legacy mode or inline mode. I recommend checking out this blog post on [Netgate's forums](#) to determine what would be the best option in your use case scenario. I selected Legacy for my use case. Go ahead and hit save.

General Settings	
Enable	<input checked="" type="checkbox"/> Checking this box enables Suricata inspection on the interface.
Interface	LAN (vtnet1) <input type="button" value="▼"/>
Choose which interface this Suricata instance applies to. In most cases, you will want to choose LAN here if this is the first Suricata-configured interface.	
Description	LAN <input type="button" value="▼"/>
Enter a meaningful description here for your reference. The default is the pfSense interface friendly description.	
Logging Settings	
Send Alerts to System Log	<input type="checkbox"/> Suricata will send Alerts from this interface to the firewall's system log. NOTE: the FreeBSD syslog daemon will automatically truncate exported messages to 480 bytes max.
Enable Stats Collection	<input type="checkbox"/> Suricata will periodically gather performance statistics for this interface. Default is Not Checked.
Enable HTTP Log	<input checked="" type="checkbox"/> Suricata will log decoded HTTP traffic for the interface. Default is Checked.
HTTP Log File Type	Regular <input type="button" value="▼"/> Select "Regular" to log to a conventional file, or choose UNIX "Datagram" or "Stream" Socket to log to an existing UNIX socket. Default is "Regular"
Append HTTP Log	<input checked="" type="checkbox"/> Suricata will append-to instead of clearing HTTP log file when restarting. Default is Checked.
Log Extended HTTP Info	<input checked="" type="checkbox"/> Suricata will log extended HTTP information. Default is Checked.
Enable TLS Log	<input checked="" type="checkbox"/> Suricata will log TLS handshake traffic for the interface. Default is Not Checked.
TLS Log File Type	Regular <input type="button" value="▼"/> Select "Regular" to log to a conventional file, or choose UNIX "Datagram" or "Stream" Socket to log to an existing UNIX socket. Default is "Regular"
Append TLS Log	<input checked="" type="checkbox"/> Suricata will append-to instead of clearing TLS log file when restarting. Default is Checked.
Enable TLS Session Resumption	<input checked="" type="checkbox"/> Suricata will output TLS transactions where the session is resumed using a Session ID. Default is Not Checked.
Enable TLS Store	<input checked="" type="checkbox"/> Suricata will log and store TLS certificates for the interface. Default is Not Checked.
Log Extended TLS Info	<input checked="" type="checkbox"/> Suricata will log extended TLS info such as fingerprint. Default is Checked.

Next let's go to the Categories tab and select the rule sets you want to enable.

Select the rulesets (Categories) Suricata will load at startup

- ▲ - Category is auto-enabled by SID Mgmt conf files
- ▲ - Category is auto-disabled by SID Mgmt conf files

[Select All](#) [Unselect All](#) [!\[\]\(7377a3302f3d0fb3a834bf90f4594228_img.jpg\) Save](#)

Enabled	Ruleset:			
Enabled	Ruleset: Default Rules	Enabled	Ruleset: ET Open Rules	Snort Rules have not been downloaded.
<input checked="" type="checkbox"/>	Snort GPLv2 Community Rules (Talos-certified)			
<input checked="" type="checkbox"/>	app-layer-events.rules	<input type="checkbox"/>	emerging-3coresec.rules	
<input checked="" type="checkbox"/>	decoder-events.rules	<input checked="" type="checkbox"/>	emerging-activex.rules	
<input checked="" type="checkbox"/>	dhcp-events.rules	<input checked="" type="checkbox"/>	emerging-adware_pup.rules	
<input checked="" type="checkbox"/>	dnp3-events.rules	<input checked="" type="checkbox"/>	emerging-attack_response.rules	
<input checked="" type="checkbox"/>	dns-events.rules	<input checked="" type="checkbox"/>	emerging-botcc.portgrouped.rules	
<input checked="" type="checkbox"/>	files.rules	<input checked="" type="checkbox"/>	emerging-botcc.rules	
<input checked="" type="checkbox"/>	ftp-events.rules	<input type="checkbox"/>	emerging-chat.rules	
<input checked="" type="checkbox"/>	http-events.rules	<input checked="" type="checkbox"/>	emerging-ciarmy.rules	
<input checked="" type="checkbox"/>	http2-events.rules	<input checked="" type="checkbox"/>	emerging-coinminer.rules	
<input checked="" type="checkbox"/>	ipsec-events.rules	<input type="checkbox"/>	emerging-compromised.rules	
<input checked="" type="checkbox"/>	kerberos-events.rules	<input checked="" type="checkbox"/>	emerging-current_events.rules	
<input checked="" type="checkbox"/>	modbus-events.rules	<input type="checkbox"/>	emerging-deleted.rules	
<input checked="" type="checkbox"/>	mqtt-events.rules	<input type="checkbox"/>	emerging-dns.rules	
<input checked="" type="checkbox"/>	nfs-events.rules	<input type="checkbox"/>	emerging-dos.rules	
<input checked="" type="checkbox"/>	ntp-events.rules	<input type="checkbox"/>	emerging-drop.rules	
<input checked="" type="checkbox"/>	quic-events.rules	<input checked="" type="checkbox"/>	emerging-dshield.rules	
<input checked="" type="checkbox"/>	rfb-events.rules	<input checked="" type="checkbox"/>	emerging-dyn_dns.rules	
<input checked="" type="checkbox"/>	smb-events.rules	<input checked="" type="checkbox"/>	emerging-exploit.rules	
<input checked="" type="checkbox"/>	smtp-events.rules	<input checked="" type="checkbox"/>	emerging-exploit_kit.rules	
<input checked="" type="checkbox"/>	ssh-events.rules	<input checked="" type="checkbox"/>	emerging-file_sharing.rules	
<input checked="" type="checkbox"/>	stream-events.rules	<input checked="" type="checkbox"/>	emerging-ftp.rules	
<input checked="" type="checkbox"/>	tls-events.rules	<input checked="" type="checkbox"/>	emerging-games.rules	

Finally, let's go back to the interfaces tab and hit the green arrow next to WAN. This should enable Suricata.

Step 6: pfSense Splunk Forwarder and Shipping of Suricata logs

In order to ship the Suricata logs to our Splunk server, we need to install a Splunk forwarder. Since pfSense is FreeBSD, we need the [Splunk Universal FreeBSD forwarder found here](#). Once that is downloaded, I found the easiest way to get it on pfSense is to unzip the .txz file and then SCP the folder to pfsense.

If you're on Mac or Linux, to extract the .txz file, run the following command:

```
tar xvzf splunkforwarder-8.0.3-a6754d8441bf-freebsd-11.1-amd64.txz
```

this system. More information on **HTTP_REFERER** is available from [Wikipedia](#).

Browser tab text Display page name first in browser tab
When this is unchecked, the browser tab shows the host name followed by the current page. Check this box to display the current page followed by the host name.

Secure Shell

Secure Shell Server Enable Secure Shell

SShd Key Only Password or Public Key
When set to *Public Key Only*, SSH access requires authorized keys and these keys must be configured for each **user** that has been granted secure shell access. If set to *Require Both Password and Public Key*, the SSH daemon requires both authorized keys and valid passwords to gain access. The default *Password or Public Key* setting allows either a valid password or a valid authorized key to login.

Allow Agent Forwarding Enables ssh-agent forwarding support.

SSH port 22
Note: Leave this blank for the default of 22.

Login Protection

Threshold 30
Block attackers when their cumulative attack score exceeds threshold. Most attacks have a score of 10.

Blocktime 120

We will be left with a few files in the directory that we unzipped the folder into. Next, we will want to scp (copy the files over SSH) the folder to our pfSense router using the following command:

```
scp -r opt/ root@ip-of-pfsense:/root/
```

While we're at it, let's unzip the Suricata TA that we downloaded earlier and scp the folder to the router as well with the following commands

```
tar xzvf splunk-ta-for-suricata_233.tgz
scp -r TA-Suricata/ root@ip-of-pfsense:/root/
```

X PROXMOX Virtual Environment 7.2-3 Search

Server View

Node 'pve'

Name ↑	Type	Active	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	Comment
enp3s0	Network Device	Yes	No	No				
enp4s0	Network Device	No	No	No				
enp5s0	Network Device	No	No	No				
vmbr0	Linux Bridge	Yes	Yes	No	enp3s0	172.19.1.101/24	172.19.1.1	

Node 'pve'

- Datacenter
- pve

- Notes
- Shell
- System
 - Network
 - Certificates
 - DNS
 - Hosts
 - Time
 - Syslog
 - Updates
 - Repositories
 - Firewall
 - Disks
 - LVM
 - LVM-Thin
 - Directory
 - ZFS
 - Ceph
 - Replication
 - Task History
 - Subscription

Logs

Having done that, we can SSH back into the router and hit option "8" for Shell. When we choose option 8, it should put us into the /root/ directory. From here, we can run an "ls" command to verify that the scp commands were successful. You should see an "opt" and "TA-Suricata" folder in /root/.

1. Let's go ahead and move the opt folder to the / directory by issuing the command:

```
mv opt/ /
```

1. Next we need to move the TA-Suricata folder to the apps folder using the following command

```
mv TA-Suricata /opt/splunkforwarder/etc/apps
```

3. Now that we have the opt directory moved and the Suricata TA in the apps folder, let's go to the Splunk forwarder folder and configure our outputs

```
cd /opt/splunkforwarder/etc/system/local
```

4. The outputs.conf file tells the Splunk forwarder where to send the data to

If there isn't a outputs.conf file in the folder, let's create one with the following content

Side note: pfSense's only text editor is Vi. Yes, I know. I'm sorry... This won't be the time or place to discuss text editors, but If you need help in Vi, there are countless guides online

```
[tcpout]
defaultGroup=my_indexers
```

```
[tcpout:my_indexers]
server=ip-of-splunk-server:9997
```

5. Next, let's configure the Suricata TA to monitor our Suricata Eve JSON log we set up earlier

6. We need to change directories to our TA-Suricata folder

```
cd /opt/splunkforwarder/etc/apps/TA-Suricata/default
```

7. Note what folder name Suricata is logging to. We can do so by ls-ing the log folder for Suricata

```
ls /var/log/suricata/
```

The screenshot shows the Splunk Enterprise interface with the following details:

- Header:** splunk>enterprise Apps ▾ Austin O'Neill ▾ 9 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find
- Page Title:** Add Data
- Left Sidebar (Tabs):**
 - Files & Directories
 - HTTP Event Collector
 - TCP / UDP** (selected)
 - Scripts
 - App Imports Update
 - App Permissions Manager
- Right Panel (TCP / UDP Configuration):**
 - Select Source: (radio button)
 - Input Settings: (radio button)
 - Review: (radio button)
 - Done: (radio button)
 - Buttons: < Back, Next >
 - Port:** 5147 (highlighted with a blue border)
 - Source name override:** optional
 - Only accept connection from:** optional

Keep note of the folder names! In my case, I have two Suricata folders inside of my Suricata log folder as I am using suricata on two interfaces. In your case, you may only have one.

8. We will now need to make/edit our inputs.conf file inside of /opt/splunkforwarder/etc/apps/TA-Suricata/default.

9. Open Vi and make the following edit:

```
[monitor:///var/log/suricata/suricata_interface_from_previous_ls_command/eve.json]
sourcetype=suricata
index=ids
host=pfSense.home
```

10. Finally, we just need to start the Splunk Forwarder. Let's change directories to the Splunk bin folder

```
cd /opt/splunkforwarder/bin
```

11. To set Splunk to start on bootup of pfSense, run

```
./splunk enable boot-start
```

12. To start Splunk run

```
./splunk start
```

Let's check out our new logs in Splunk

```
index=ids sourcetype=suricata*
```

Splunk > enterprise App: Search & ... Austin O'Neil 9 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

New Search

Save As Close

1 index=network sourcetype=pfsense* host="pfSense.home"

Last 24 hours

404,061 of 404,061 events matched No Event Sampling Job II □ ▶ ↻ ↻ Verbose Mode

Events (404,061) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection × Deselect 1 hour per column

May 5, 2020 6:00 AM

	List	Format	20 Per Page	< Prev	1	2	3	4	5	6	7	8	...	Next >	
◀ Hide Fields	☰ All Fields	i Time	Event												
SELECTED FIELDS		> 5/5/20 8:00:26.000 PM	May 6 00:00:26 filterlog: 5,,,100000003,em0,match,block,in,6,0x00,0x0000,255,UDP,17,391,fe80::147a:370:ab0e:a2f1,ff02::fb,5353,5353,391 host = pfSense.home source = pfSense.home sourcetype = pfsense:filterlog												
a host 1		> 5/5/20 8:00:26.000 PM	May 6 00:00:26 filterlog: 69,,,100000101,em0,match,pass,in,4,0x0,,32,0,0,none,17,udp,411,10.10.10.20,224.0.0.251,5353,5353,391 host = pfSense.home source = pfSense.home sourcetype = pfsense:filterlog												
a source 1		> 5/5/20 8:00:26.000 PM	May 6 00:00:26 filterlog: 54,,,1000005911,igb0,match,pass,out,4,0x0,,63,0,0,DF,1,icmp,84,24.144.179.56,8.8.8.8,request,12822,164 host = pfSense.home source = pfSense.home sourcetype = pfsense:filterlog												
a sourcetype 3		> 5/5/20 8:00:26.000 PM	May 6 00:00:26 filterlog: 76,,,1585512506,em0.40,match,pass,in,4,0x0,,64,0,0,DF,1,icmp,p,84,10.40.0.16,8.8.8.8,request,1620,164 host = pfSense.home source = pfSense.home sourcetype = pfsense:filterlog												
INTERESTING FIELDS		> 5/5/20 8:00:26.000 PM	May 6 00:00:26 filterlog: 75,,,1585662439,em0.40,match,block,in,4,0x0,,64,0,0,DF,6,tcpc,64,10.40.0.43,10.10.10.20,50260,65013,0,S,3697425533,,65535,,mss;nop;wscale;nop;nop;TS;sackOK;eol host = pfSense.home source = pfSense.home sourcetype = pfsense:filterlog												
a action 2		> 5/5/20 8:00:26.000 PM	May 6 00:00:26 filterlog: 5,,,100000003,em0.40,match,block,in,6,0x00,0xd52b2,255,UDP,17,183,fe80::1431:2b6:510c:a8ad,ff02::fb,5353,5353,183 host = pfSense.home source = pfSense.home sourcetype = pfsense:filterlog												
a app 1		> 5/5/20 8:00:26.000 PM	May 6 00:00:26 filterlog: 76,,,1585512506,em0.40,match,pass,in,4,0x0,,255,31334,0,none,17,udp,203,10.40.0.43,224.0.0.251,5353,5353,183 host = pfSense.home source = pfSense.home sourcetype = pfsense:filterlog												
# bytes 100+		> 5/5/20 8:00:25.000 PM	May 6 00:00:25 filterlog: 53,,,1000005813,em0.40,match,pass,out,4,0x0,,63,28622,0,DF,6,tcp,60,10.10.10.10.40.0.4,49640,80,0,S,136372809,,64240,,mss;sackOK;TS;nop;wscale host = pfSense.home source = pfSense.home sourcetype = pfsense:filterlog												
# bytes_in 100+		> 5/5/20 8:00:25.000 PM	May 6 00:00:25 filterlog: 69,,,100000101,em0,match,pass,in,4,0x0,,64,28622,0,DF,6,tcp,60,10.10.10.10.40.0.4,49640,80,0,S,136372809,,64240,,mss;sackOK;TS;nop;wscale host = pfSense.home source = pfSense.home sourcetype = pfsense:filterlog												
# bytes_out 100+		> 5/5/20	May 6 00:00:25 filterlog: 76,,,1585512506,em0.40,match,pass,in,4,0x0,,64,0,0,DF,1,icmp												
# date_hour 16															
# date_mday 2															
# date_minute 60															
a date_month 1															
# date_second 60															
a date_wday 2															
# date_year 1															
a date_zone 1															
a dest 100+															
a dest_int 5															
a dest_ip 100+															
a dest_is_expected 1															
a dest_pci_domain 1															
# dest_port 100+															
a dest_requires_av 1															
a dest_should_timesync 1															
a dest_should_update 1															
a direction 2															
a eventtype 4															
a flags 2															
# id 100+															
a index 1															
# ip_version 2															
# linecount 1															
# offset 1															
...															

Great! As you can see, we are now receiving extracted Suricata logs being returned from our search. Since we installed the CIM app, we can do stuff like tag=dns and receive back DNS logs and so forth. Again, if you don't see all interesting fields on the left, be sure to run your search in "Verbose" mode.

Create Alerts

- in splunk go to search
- index=ids | spath dest_port | search dest_port=8888| spath "http.url" | search "http.url"="/beacon"
- Save as → alert
- set parameters: run every hour if number of results > 5, add to triggered alerts

Download abuse.ch feeds

- Add a data input for splunk: in splunk settings → data input -> files and directories
 - /root/abuse
 - denylist: *.csv
 - host: [abuse.ch](#)
 - index: abuse_ch
- python script to fetch feeds (in /root/abuse)

```

# Import necessary libraries
import requests
from pathlib import Path
from zipfile import ZipFile
from dataclasses import dataclass

@dataclass
class Feed:
    recent_path: Path
    full_feed_path: Path
    recent_feed_url: str
    full_feed_url: str

def fetch_csv_feed(feed: Feed) -> None:
    """
    Fetches the CSV feed from the provided URL and saves it to the specified path.

    If the CSV file already exists, it fetches the recent CSV feed. Otherwise, it fetches the full CSV feed,
    extracts the contents of the zip file, and renames the extracted CSV file to the original CSV file name.

    Args:
        feed (Feed): An instance of the Feed dataclass.

    Returns:
        None
    """
    # Check if the CSV file already exists
    if feed.recent_path.exists():
        # If it exists, fetch the recent CSV feed
        response = requests.get(feed.recent_feed_url)
        # Write the response content to the CSV file
        with feed.recent_path.open("wb") as file:
            file.write(response.content)
    else:
        # If it doesn't exist, fetch the full CSV feed
        response = requests.get(feed.full_feed_url)
        # Create a zip file path by appending ".zip" to the CSV file path
        zip_file = feed.recent_path.with_suffix(".zip")
        # Write the response content to the zip file
        with zip_file.open("wb") as file:
            file.write(response.content)

        # Extract the contents of the zip file to the parent directory of the CSV file
        with ZipFile(zip_file, "r") as zip_ref:
            zip_ref.extractall(feed.recent_path.parent)

        # Delete the zip file
        zip_file.unlink()

    # Rename the extracted CSV file to the original CSV file name
    feed.full_feed_path.rename(feed.recent_path)

def main():
    # Get the current working directory
    current_directory = Path(".")

    # Create feeds
    feeds = [
        # threatfox
        Feed(
            current_directory / "threatfox.csv",

```

```
    current_directory / "full.csv",
    "https://threatfox.abuse.ch/export/csv/recent/",
    "https://threatfox.abuse.ch/export/csv/full/",
),
# malwarebazaar
Feed(
    current_directory / "malwarebazaar.csv",
    current_directory / "full.csv",
    "https://bazaar.abuse.ch/export/csv/recent/",
    "https://bazaar.abuse.ch/export/csv/full/",
),
# URLhaus
Feed(
    current_directory / "urlhaus.csv",
    current_directory / "csv.txt",
    "https://urlhaus.abuse.ch/downloads/csv_recent/",
    "https://urlhaus.abuse.ch/downloads/csv/",
),
],
]

# Fetch the CSV feeds
for feed in feeds:
    fetch_csv_feed(feed)

if __name__ == "__main__":
    main()
```

use crontab to fetch the feeds automatically every hour

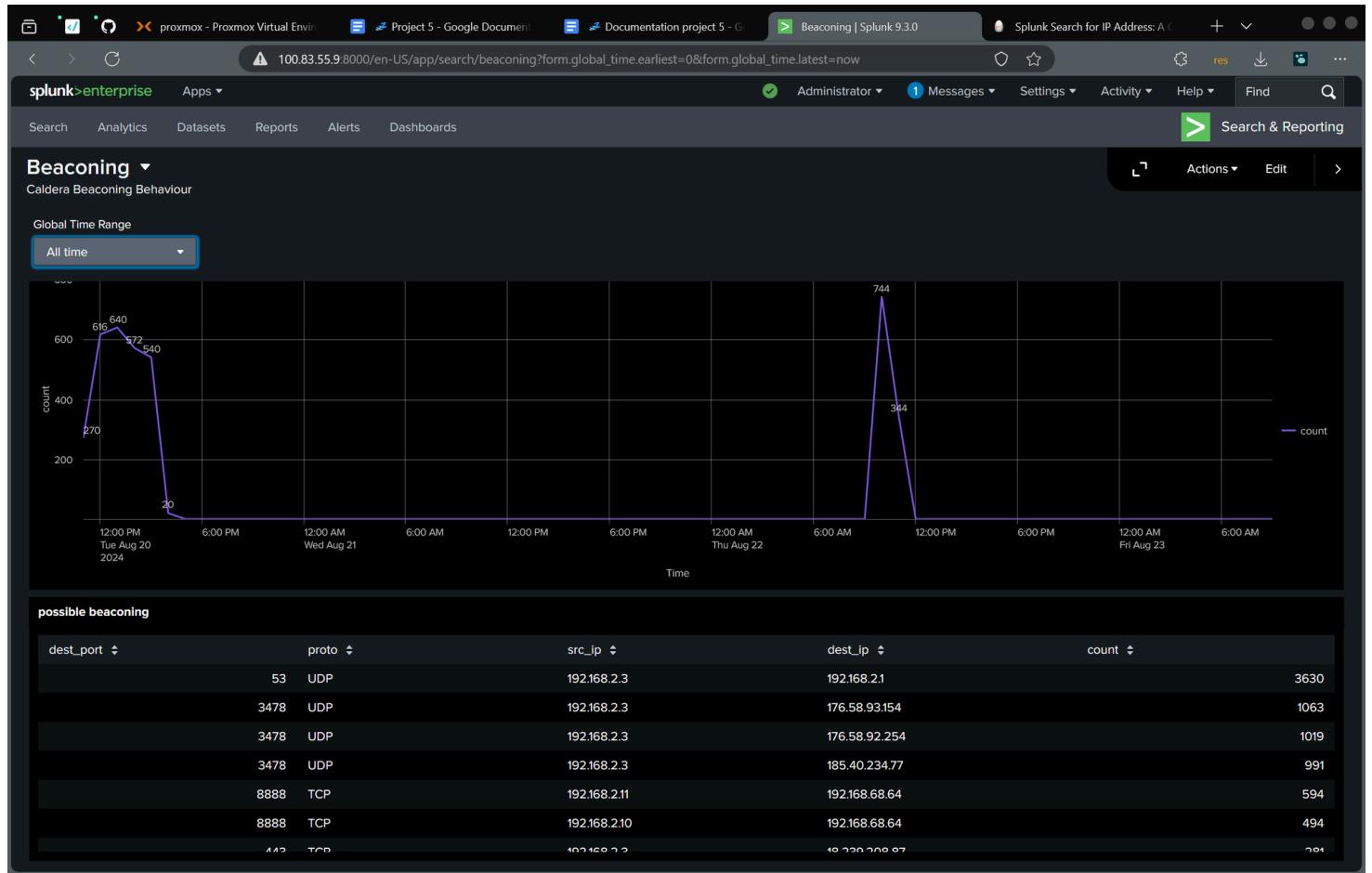
```
crontab -e
```

```
0 * * * * /usr/bin/python3 /root/abuse/download_feeds.py
```

Dashboard Creation

- Go to dashboards → create new dashboard
- add line chart
- data sources: index=ids| spath dest_port | search dest_port=8888 | timechart count span=1h
- X axis = time, y-axis = count
- add another panel with

```
index=ids source="/var/log/suricata/pfsense/suricata_vtnet155920/eve.json" | regex src_ip="192\.168\.2\.\d{1,3}" | stats count by dest_port pr as search query for possible beaconing
```



Add Report Correlating threatfox ports to suricata logs

- open search
- ```
index="abuse_ch" source="/root/abuse/threatfox.csv" | where ioc_type = "ip:port" | rex field=ioc_value ".*:(<port>.*)" | stats count by port,t
```
- save as → report

# Caldera

Caldera is an open-source cybersecurity platform designed to automate adversary emulation, assist manual red teams, and facilitate incident response. It leverages the MITRE ATT&CK framework to simulate real-world cyberattacks, helping organizations identify vulnerabilities and improve their security posture.

## Installation on kali

```
apt install caldera
vi /etc/systemd/system/caldera.service
```

```
[Unit]
Description=Caldera Service
After=network.target
```

```
[Service]
User=root
Group=root
ExecStart=/usr/bin/caldera
Restart=always
```

```
[Install]
WantedBy=multi-user.target
```

```
systemctl enable --now caldera
```

## Agents

### 1. Access the CALDERA Web Interface

- Open your web browser and navigate to the CALDERA web interface.
- Log in with your credentials.

### 2. Navigate to the Agents Tab

- From the dashboard, click on the "Agents" tab in the navigation menu.

### 3. Select and Install Agents

- In the Agents tab, you'll see different types of agents available for installation.
- Select the agent you want to deploy. Typically, this involves downloading a preconfigured script or executable.

### 4. Deploy the Agent

- On the target machine where you want to install the agent, download the script or executable provided.
- Run the script or executable as instructed on the target machine. This will install the agent and establish a connection back to the CALDERA server.

### 5. Verify Agent Installation

- Return to the CALDERA web interface and check the Agents tab.
- The newly installed agent should appear in the list, showing its status (e.g., active or idle).
- You can now use this agent to simulate adversarial behaviour or collect data.

### 6. Manage and Configure Agents

- Once the agent is installed, you can manage its settings directly from the CALDERA interface.
- This might include configuring the agent's behaviour, assigning it to specific operations, or monitoring its activity.

## **7. Use Agents in Operations**

- After installing the agents, you can use them in various CALDERA operations.
- Navigate to the "Operations" tab, create a new operation, and assign the agent to carry out tasks according to your needs.

# PfSense

pfSense is an open-source customized distribution of FreeBSD, designed specifically for use as a firewall and router. It is widely recognized for its robustness and flexibility, offering enterprise-grade network security features that are fully managed through an intuitive web interface. pfSense is commonly used in both small-scale and enterprise environments to secure network infrastructures, manage traffic, and enforce security policies.

## Installation

First create two Linux Bridges on Proxmox VE, which will be used for LAN and WAN on the firewall VM.

Select the host from the server view

Navigate to System -> Network

This example uses enp4s0 and enp5s0 interfaces for the firewall, while enp3s0 is for Proxmox VE management. The naming of interfaces will vary depending on the hardware involved (interface type, bus location, etc.).

The screenshot shows the Splunk Enterprise interface with the 'Indexes' dashboard. A modal window titled 'New Index' is open, prompting for configuration details. The 'General Settings' section includes fields for 'Index Name' (set to 'network'), 'Index Data Type' (selected as 'Events'), 'Home Path' (set to 'optional'), 'Cold Path' (set to 'optional'), 'Thawed Path' (set to 'optional'), 'Data Integrity Check' (set to 'Enable'), 'Max Size of Entire Index' (set to '500 GB'), 'Max Size of Hot/Warm/Cold Bucket' (set to 'auto'), 'Frozen Path' (set to 'optional'), and an 'App' dropdown set to 'Enterprise Security'. The 'Storage Optimization' section contains a 'Tsidx Retention Policy' toggle ('Enable Reduction') with a warning message about the potential risks of reduction. Below it is a 'Reduce tsidx files older than' field with a 'Days' dropdown. At the bottom right of the modal are 'Save' and 'Cancel' buttons. The background shows a list of existing indexes with names like '\_audit', '\_internal', '\_introspection', '\_metrics', '\_telemetry', '\_thefishbucket', 'cim\_modactions', 'cisco', 'docker', 'endpoint\_summary', 'gia\_summary', and 'haproxy'.

Click Create

Select Linux Bridge

Enter enp4s0 under Bridge ports

The screenshot shows the Splunk interface with the title 'Add new'. Below it, the path 'Forwarding and receiving > Receive data > Add new' is visible. The main section is titled 'Configure receiving' with the sub-instruction 'Set up this Splunk instance to receive data from forwarder(s.)'. A field labeled 'Listen on this port \*' contains the value '9997'. A note below the field says 'For example, 9997 will receive data on TCP port 9997.' At the bottom right are 'Cancel' and 'Save' buttons.

Repeat the process to add another Linux Bridge, this time add enp5s0 under Bridge ports.

The screenshot shows a 'Create: Linux Bridge' dialog box. It has fields for 'Name' (vmbr2), 'Autostart' (checked), 'Bridge ports' (enp5s0), and other networking parameters like IPv4/CIDR, Gateway (IPv4), and IPv6/CIDR. At the bottom are 'Help', 'Advanced' (unchecked), and a prominent 'Create' button.

Click Apply Configuration to configure the new interfaces in the OS

Click Yes to confirm the action

Proxmox VE networking should now display two Linux bridges like on the following screenshot.

#### Note

If the interfaces do not show as Active, reboot the Proxmox VE host.

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for 'Austin O'Neil', 'Messages' (9 notifications), 'Settings', 'Activity', 'Help', and a search bar. Below the navigation, the main title is 'Upload app' with a breadcrumb trail 'Apps > Upload app'. The central content area has a white background with a form titled 'Upload an app'. It instructs users to upload a .spl or .tar.gz file. A file input field shows 'ta-pfsense\_221.tgz' has been selected. There's also a checkbox for upgrading an existing app. At the bottom are 'Cancel' and 'Upload' buttons.

## Configuration

### 1. Prepare VirtualBox Networks

- **Create Network Interfaces:**
  - **NAT Network (WAN):** Use the default NAT network.
  - **Internal Network (LAN):** Create a new internal network called "intnet".
  - **Internal Network (OPT1):** Create another internal network called "opt1".

### 2. Create pfSense Virtual Machine

- **New VM:**
  - **Name:** pfSense
  - **Type:** BSD
  - **Version:** FreeBSD (64-bit)
  - **Memory Size:** 1024 MB (1 GB)
  - **Hard Disk:** Create a new virtual hard disk (20 GB).
- **Network Adapters:**
  - **Adapter 1:** Attached to NAT.
  - **Adapter 2:** Attached to Internal Network "intnet".
  - **Adapter 3:** Attached to Internal Network "opt1".

### 3. Install pfSense

- **Start the VM:**
  - Attach the pfSense ISO as the optical drive.
  - Boot the VM to start the pfSense installer.
  - Proceed with the default installation options.
- **Partitioning:**
  - Choose "Auto (UFS)" for the partitioning method.
  - After installation, remove the ISO and reboot the VM.

### 4. Initial Setup and Interface Assignment

- **Console Configuration:**
  - Assign interfaces: Typically `em0` for WAN, `em1` for LAN, and `em2` for OPT1.
  - Set up the IP address for the LAN interface (default is `192.168.1.1`).

## 5. Access pfSense Web Interface

- **Connect to LAN:**
  - Open a web browser on a machine connected to the "intnet" network.
  - Go to <https://192.168.1.1>.
  - Log in using the default credentials ( `admin / pfsense` ).

## 6. WebConfigurator Setup Wizard

- **General Setup:**
  - Configure hostname, domain, and DNS settings.
- **Time Server:**
  - Set the time zone for your location.
- **WAN Configuration:**
  - Leave as default if using DHCP on the WAN side.
- **LAN Configuration:**
  - Set the LAN IP and subnet.
- **Admin Password:**
  - Change the default admin password for security.

## 7. Configure OPT1 Interface

- **Interface Setup:**
  - Go to `Interfaces > OPT1`, enable the interface, and assign a static IP (e.g., `192.168.2.1`).
- **DHCP Server:**
  - Enable the DHCP server for the OPT1 interface under `Services > DHCP Server`.
  - Define a range for IP assignments (e.g., `192.168.2.100` to `192.168.2.200` ).

## 8. Firewall Rules

- **Create Rules:**
  - Go to `Firewall > Rules`.
  - Create rules for LAN and OPT1 to allow traffic.

## 9. Testing the Setup

- **Client Configuration:**
  - Create a new VM in VirtualBox and connect it to the "intnet" network for LAN testing.
  - Create another VM connected to "opt1" for OPT1 testing.
  - Ensure both VMs can access the internet via the pfSense firewall.

## 10. Final Adjustments

- **Security Hardening:**
  - Consider setting up VPNs, VLANs, and additional firewall rules as needed.
  - Regularly update pfSense for security patches.

# Suricata

Suricata is an open-source, high-performance network intrusion detection and prevention system (IDS/IPS). It's capable of real-time traffic inspection at high speeds, making it suitable for large-scale networks. Suricata uses a combination of signature-based and anomaly-based detection techniques to identify malicious activity.

## Installation on pfSense

System → package manager → suricata

### Forward suricata logs to splunk with cron and rsync

- Set up ssh keys for passwordless login to splunk

```
ssh-keygen
ssh-copy-id -i .ssh/id_rsa.pub root@192.168.2.3
```

- install rsync

```
pkg install rsync
```

- Use the cron package to send the logs to splunk

```
crontab -e
```

```
/15 * * * /usr/local/bin/rsync --recursive --delete-after --compress /var/log/suricata/ root@192.168.2.3:/var/log/suricata/pfSense/
```

- in splunk settings → data input -> files and directories
  - /var/log/suricata/pfSense
  - app context: TA-suricata
  - host: pfSense
  - index: ids

## Configuring Suricata on pfSense

- Next, we want to go to the “Updates” tab and hit “Force” to force download all the rules we selected on the previous page.
- Once that is done, we can return to the Interfaces tab and click the “+ Add” button to set up the LAN interface. There will be a few screenshots below—these are what I determined to give the best logging output. We need Suricata to log in EVE JSON mode.

The screenshot shows a configuration dialog for creating a Linux bridge. The fields are as follows:

|                 |       |               |                                     |
|-----------------|-------|---------------|-------------------------------------|
| Name:           | vmbr1 | Autostart:    | <input checked="" type="checkbox"/> |
| IPv4/CIDR:      |       | VLAN aware:   | <input type="checkbox"/>            |
| Gateway (IPv4): |       | Bridge ports: | enp4s0                              |
| IPv6/CIDR:      |       | Comment:      |                                     |
| Gateway (IPv6): |       |               |                                     |

At the bottom, there are buttons for Help, Advanced, and Create.

Next let's go to the Categories tab and select the rule sets you want to enable.

**splunk>enterprise** App: Search & R... ▾ Austin O'Neil ▾ 9 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As ▾ Close

1 index=ids sourcetype=suricata\* host=pfSense.home Last 24 hours ▾

97,017 of 97,017 events matched No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (97,017) Patterns Statistics Visualization Format Timeline ▾ 1 hour per column

| List ▾             |  |            |  | Format                   | 20 Per Page ▾                                                                                                                                                                                                                                                                                                                                                                                                                                    | < Prev | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | ... | Next > |  |  |
|--------------------|--|------------|--|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|---|---|---|---|---|---|---|-----|--------|--|--|
| < Hide Fields      |  | All Fields |  | i Time                   | Event                                                                                                                                                                                                                                                                                                                                                                                                                                            |        |   |   |   |   |   |   |   |   |     |        |  |  |
| SELECTED FIELDS    |  |            |  | > 5/5/20 10:43:28.298 PM | <pre>{   [-]     dest_ip: 10.10.0.1     dest_port: 53     dns: { [+]       }       event_type: dns       flow_id: 766922854534973       in_iface: igb0       proto: UDP       src_ip: 24.144.179.56       src_port: 13668       timestamp: 2020-05-05T22:43:28.298813-0400     }     Show as raw text     host = pfSense.home   source = /var/log/suricata/suricata_igb06761/eve.json       sourcetype = suricata:dns   </pre>                   |        |   |   |   |   |   |   |   |   |     |        |  |  |
| INTERESTING FIELDS |  |            |  | > 5/5/20 10:43:27.766 PM | <pre>{   [-]     dest_ip: 172.217.9.67     dest_port: 80     event_type: http     flow_id: 2226522383933030     http: { [+]       }       in_iface: igb0       proto: TCP       src_ip: 24.144.179.56       src_port: 20500       timestamp: 2020-05-05T22:43:27.766923-0400       tx_id: 7     }     Show as raw text     host = pfSense.home   source = /var/log/suricata/suricata_igb06761/eve.json       sourcetype = suricata:http   </pre> |        |   |   |   |   |   |   |   |   |     |        |  |  |
|                    |  |            |  | > 5/5/20 10:43:27.766 PM | <pre>{   [-]     ...   </pre>                                                                                                                                                                                                                                                                                                                                                                                                                    |        |   |   |   |   |   |   |   |   |     |        |  |  |

# Detecting encrypted beacons

## Caldera

### SSL

#### Setup Instructions

Note: OpenSSL must be installed on your system to generate a new self-signed certificate

- In the root CALDERA directory, navigate to plugins/ssl.
- Place a PEM file containing SSL public and private keys in conf/certificate.pem. Follow the instructions below to generate a new self-signed certificate:
- In a terminal, paste the command:

```
openssl req -x509 -newkey rsa:4096 -out conf/certificate.pem -keyout conf/certificate.pem -nodes
```

This will prompt you to identify details. Enter your country code when prompted. You may leave the rest blank by pressing enter.

- Copy the file haproxy.conf from the templates directory to the conf directory.
- Open the file conf/haproxy.conf in a text editor.
- On the line `bind *:8443 ssl crt plugins/ssl/conf/insecure_certificate.pem`, replace `insecure_certificate.pem` with `certificate.pem`.
- On the line `server caldera_main 127.0.0.1:8888 cookie caldera_main`, replace `127.0.0.1:8888` with the host and port defined in CALDERA's conf/local.yml file. This should not be required if CALDERA's configuration has not been changed.
- Save and close the file. Congratulations! You can now use CALDERA securely by accessing the UI `https://<YOUR_IP>:8443` and redeploying agents using the HTTPS service.
- install haproxy

```
apt install haproxy
cd /var/lib/caldera/plugins/ssl
openssl req -x509 -newkey rsa:4096 -out conf/certificate.pem -keyout conf/certificate.pem -nodes
cp templates/haproxy.conf conf/
nano conf/haproxy.conf
```

- find `bind *:8443 ssl crt plugins/ssl/conf/insecure_certificate.pem` and change to `certificate.pem`
- remove nbproc line
- run `haproxy -f haproxy.conf` to check for errors
- access caldera on port 8443 over https

## Deploy https agents

don't forget to add k flag to ignore self-signed certificate

```
curl -k -s -X POST -H "file:sandcat.go" -H "platform:linux" $server/file/download > splunkd
```

## Zeek

### 1. Access the pfSense Web Interface

Log into your pfSense web interface using your browser.

### 2. Navigate to the Package Manager

Go to System -> Package Manager. In the Package Manager, click on the "Available Packages" tab.

### 3. Install Zeek

Search for "Zeek" in the available packages list. Click the + Install button next to Zeek to begin the installation process. Confirm the installation and wait for it to complete.

### 4. Configure Zeek

After installation, navigate to Services -> Zeek to configure and start Zeek. Customize Zeek settings according to your network monitoring needs.

### 5. Start Zeek

Enable and start the Zeek service. Review logs and performance to ensure Zeek is operating correctly on your network.

## Enable ja4 fingerprinting

- install ja4 package and enable script dir

```
zkg autoconfig
zkg install zeek/foxio/ja4
```

- set up crontab to send logs to splunk

```
crontab -e
```

```
*/15 * * * * /usr/local/bin/rsync --recursive --delete-after --compress /usr/local/logs/current/ root@192.168.2.3:/var/log/zeek/pfsense
```

## Splunk Setup

- install TA for zeek: <https://splunkbase.splunk.com/app/5466>
- add data input in splunk:
  - settings → data inputs → files and directories → new
  - directory: /var/log/zeek/pfsense
  - source type: zeek
  - includelist: .\*log
  - index: zeek
- search for beaconing

```
index="zeek" sourcetype=zeek:ssl
| eval ja4_a=mvindex(split(ja4,"*"),0)
| eval alpn = substr(ja4_a, -2, 2)
| eval ja4s_a=mvindex(split(ja4s,"*"),0)
| eval server_alpn = substr(ja4s_a, -2, 2)
| where alpn == "00" or server_alpn = "00"
| stats count, values(id_orig_h) as id_orig_h_values, values(id_resp_h) as id_resp_h_values, values(ja4) as ja4_values, values(ja4s) as ja4s_values
| sort -count
| table count, server_name, id_orig_h_values, id_resp_h_values, ja4_values, ja4s_values
```