

# Transparent Proxy with Suricata

---

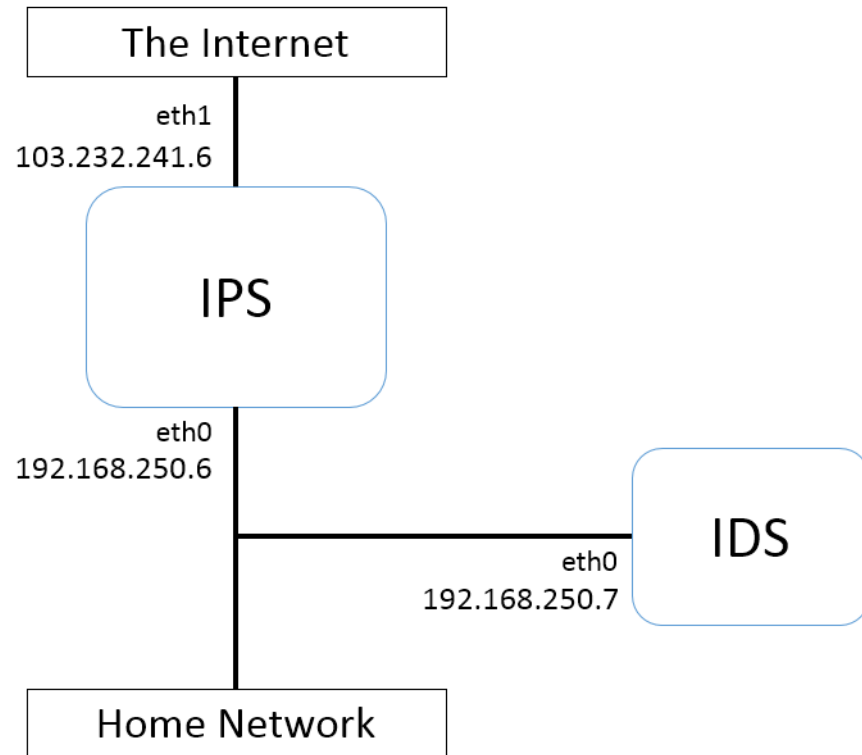
AJAY BRAHMAKSHATRIYA (CS12B1004)

BHATU PRATIK (CS12B1010)

ADVISOR: PRAKASH PAWAR

# Network Diagram

---



- Two Installations of Suricata
- First running on the same machine as the squid proxy, working in IPS mode.
- Second getting the mirrored traffic for running in IDS mode.
- All traffic from home network reaches the second machine.

# Mirror Traffic to IDS Machine

---

We want to send all data coming to IPS machine to IDS machine before it gets processed for both incoming and outgoing.

Enter:

```
iptables -I PREROUTING -t mangle -i eth0 -j TEE --gateway 192.168.250.7
```

```
iptables -I POSTROUTING -t mangle -j TEE --gateway 192.168.250.7
```

# Configure Squid

---

We configure squid server in IPS Machine (192.168.250.6:3129)

Reason: Direct home traffic to IPS Machine.

No caching.

Alternative: Routing rules in campus network.

**Future:** No Squid – Install Suricata in Gateway Router

# Log Comparison

---

**Squid Log:** /var/log/squid3/access.log - **Suricata Log:** /var/log/suricata/http.log

No. of requests logged are same. Sample:

## Squid Log

```
424467883.995 263 172.16.3.43 TCP MISS/200 2675 GET http://upload.wikimedia.org/wikipedia/meta/2/27/Wikisource-logo sister 1x.png - HIER  
DIRECT/208.80.154.240 image/png  
  
1424467884.287 263 172.16.3.43 TCP MISS/200 1869 GET http://upload.wikimedia.org/wikipedia/meta/a/af/Wikiversity-logo sister 1x.png - HIER  
DIRECT/208.80.154.240 image/png
```

## Suricata Log

```
02/21/2015-03:01:23.994598 upload.wikimedia.org [**] /wikipedi-a/meta/2/27/Wikisource-logo sister 1x.png [**] Mozilla/5.0(Windows NT 6.3; WOW64)  
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.111 Safari/537.36 [**] 103.232.241.6:40958- > 208.80.154.240:80  
  
02/21/2015-03:01:24.286601 upload.wikimedia.org [**] /wikipedi-a/meta/a/af/Wikiversity-logo sister 1x.png [**] Mozilla/5.0(Windows NT 6.3; WOW64)  
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.111 Safari/537.36 [**] 103.232.241.6:40958 - > 208.80.154.240:80
```

# Formal Log Comparison

---

Python Script to Compare logs:

We compare hits for domain names in each log and output the domain names that are in squid log[`access.log`] and not in Suricata log[`http.log`].

Results:

On comparing a session of 30 minutes with around 5000 requests we see that the output is empty i.e. there is no connection that Suricata misses. It monitors every connection.

# Documentation

1

# Buricata with Transport Proxy

Alex Frohnholtz  
Frodo Baggins  
@0x00sec

**About**

The document describes the process of configuring Buricata to intercept incoming traffic and redirect it through a transport proxy. It will contain some details but will leave out most of the configuration of the proxy itself as well as the configuration of the proxy server.

This manual is meant to be referenced by help network administrators configure Buricata for listening and directing incoming traffic. It contains knowledge which would help in setting system configurations.

## Contents

- Overview
- Installing Buricata 2.0.6.7 to Ubuntu
- Notes
- Configuration
- Execution
  - Starting .....
  - Logging .....
- Installing IIS/IIS Server for Logging
- Testing and Troubleshooting

---

Copyright © 2012-2013 Alex Frohnholtz

3

[illegible]

5

[illegible]

7

[illegible]

2

<b>Overview</b>	
<b>What is assessed:</b>	<p>It is an Extension Discussion and Formative response. It represents the outcome of IED (Interpretation) and IED Extension. It presents a statement of working notes on the flow chart. This enables a single Result and/or an Interpretation of the water sampling to be made. It is a summary of the water sampling results and flow chart. It is a valuable response that is used in the IED and is critical to completing the IED.</p> <p>It is a summary of the water sampling results and flow chart. It is a valuable response that is used in the IED and is critical to completing the IED.</p>
<b>IED Model</b>	<p>The IED Model is a summary of the water sampling results and flow chart. It is a valuable response that is used in the IED and is critical to completing the IED.</p>
<b>IED Model</b>	<p>The IED Model is a summary of the water sampling results and flow chart. It is a valuable response that is used in the IED and is critical to completing the IED.</p>
<b>Configuration:</b>	<p>The configuration for the IED is a summary of the water sampling results and flow chart. It is a valuable response that is used in the IED and is critical to completing the IED.</p>
<b>Notes</b>	<p>The notes are used to record the water sampling results and flow chart. It is a valuable response that is used in the IED and is critical to completing the IED.</p>
<b>Logic</b>	<p>The logic is used to record the water sampling results and flow chart. It is a valuable response that is used in the IED and is critical to completing the IED.</p>
<b>2. Installing Service Data</b>	<p>The Service Data is a summary of the water sampling results and flow chart. It is a valuable response that is used in the IED and is critical to completing the IED.</p>

4

[illegible]

6

[illegible]

8

[illegible]