Adaptación del IDS/IPS Suricata para que se pueda convertir en una solución empresarial.

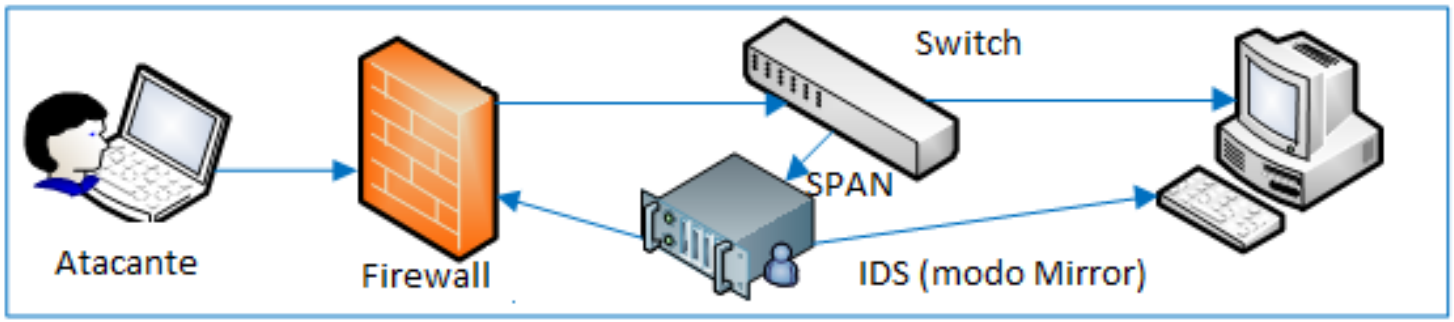
-Juan Astudillo
- Alberto Jimenez
- Fernando Ortiz

Agenda

- Antecedentes y Objetivos
- Descripción del Estado Actual del IDS/IPS Suricata
- Diseño e implementación de la solución IDS/IPS Empresarial
- Diseño e integración del módulo de detección de anomalías
- Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías
- Propuestas de mejoras para la solución empresarial actual
- Conclusiones y recomendaciones

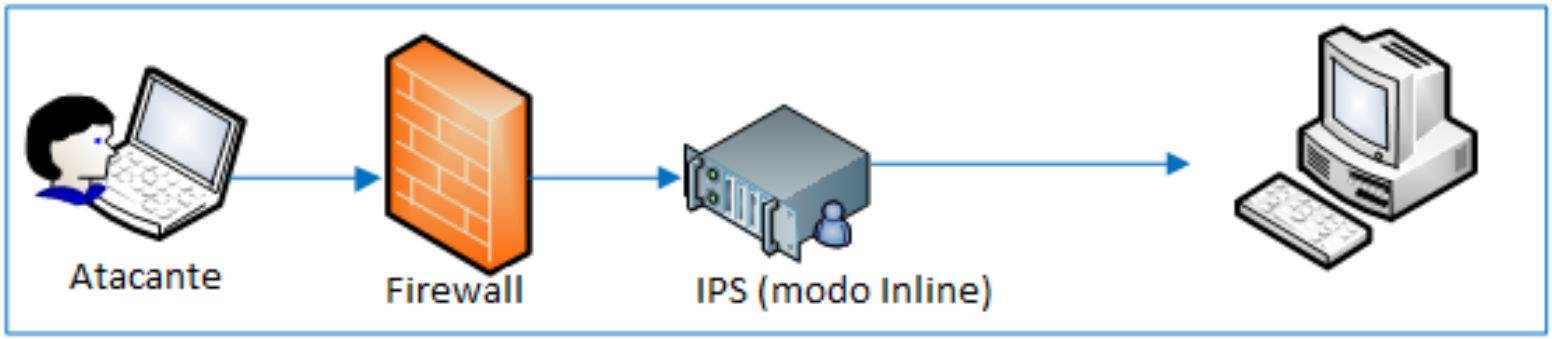
Antecedentes y Objetivos

- Sistemas de Detección de Intrusos (IDS)
  - Dispositivo de red que **detecta** accesos no autorizados y ataques de red.
  - Respuesta Pasiva
  - Alertas
  - Modo Mirror
- .



Antecedentes y Objetivos

- Sistemas de Prevención de Intrusos (IPS)
  - Dispositivo que ejerce **control de acceso** de una red informática para proteger los sistemas computacionales
  - Respuesta Activa
  - Mitiga, bloquea, previene
  - Modo Inline



Antecedentes y Objetivos

- Modos de detección de los ataques IDS/IPS
  - **Basados en Firmas**
  - Basados en Políticas
  - Basados en Anomalías

Antecedentes y Objetivos

- Diferencias entre IDS/IPS

	IPS	IDS
	Inline, Bloque Automático	**Mirror, Alertas para analistas**
Estabilidad de la red	Caída del sistema es catastrófica para la red	Caída del sistema quita información al analista de red. No es algo crítico
Desempeño	Requiere mayor capacidad de procesamiento. Puede producir cuellos de botella.	La falta de procesamiento puede ser compensada con buffers de mucha memoria. Nunca producirá cuellos de botella.
Precisión de Falsos Positivos	Produce bloqueos de paquetes. Problema con aplicaciones.	Carga trabajo innecesaria para el analista en busca de falsas alarmas.
Precisión de Falsos Negativos	Paquetes maliciosos entran a la red. No es tan crítico como en el caso de los IDS.	Ataques resultan totalmente **invisibles** y pueden volver a ocurrir. Pérdida de información para el analista.

Tabla 1.1: Diferencias entre IDS e IPS

Antecedentes y Objetivos

- La Actualidad en los IDS/IPS
  - La cifra del mercado mundial de los IPS creció en 5% en el 2010. (Gartniar Magic Quadrant)
  - Técnicas de detección por anomalías permiten detectar nuevos tipos de ataques.
  - Se está aplicando detección de intrusos para dispositivos móbiles.

Antecedentes y Objetivos

- Justificación
  - Los sistemas IDS/IPS empresariales son muy costosos.
  - Snort como Suricata no son soluciones empresariales.
  - Es necesario integrarlo con módulos externos
  - La contínua actividad desarrolladora de Suricata y planes a futuro han hecho del proyecto el favorito de muchos desarrolladores.

Objetivos de la Tesis

- Definir el estado de arte actual del proyecto.
- Someter al IDS/IPS a pruebas de rendimiento, para identificar sus verdaderas capacidades.
- Desarrollar la interfaz de administración.
- Desarrollar un módulo de anomalías y autoaprendizaje.

Agenda

- Antecedentes y Objetivos
- Descripción del Estado Actual del IDS/IPS Suricata
- Diseño e implementación de la solución IDS/IPS Empresarial
- Diseño e integración del módulo de detección de anomalías
- Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías
- Propuestas de mejoras para la solución empresarial actual
- Conclusiones y recomendaciones

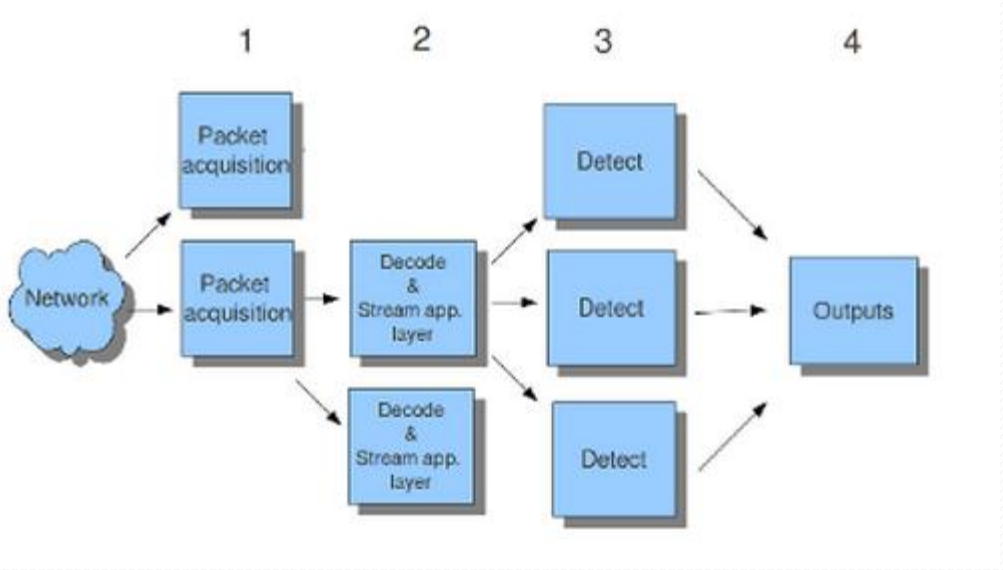
Descripción y Estado actual del IDS/IPS Suricata

- Descripción y Carácterísticas de Suricata
  - **Multi-threading**
  - Estadísticas de Rendimiento
  - Detección de protocolos automático
  - Métodos de Entrada Estándar (libpcap, pfring, nfqueue)
  - **IP Reputation**
  - Geolocalización
  - Aceleración por GPU
  - Soporte para IPv6
  - Compatibilidad con Soluciones para Snort

Descripción y Estado actual del IDS/IPS Suricata

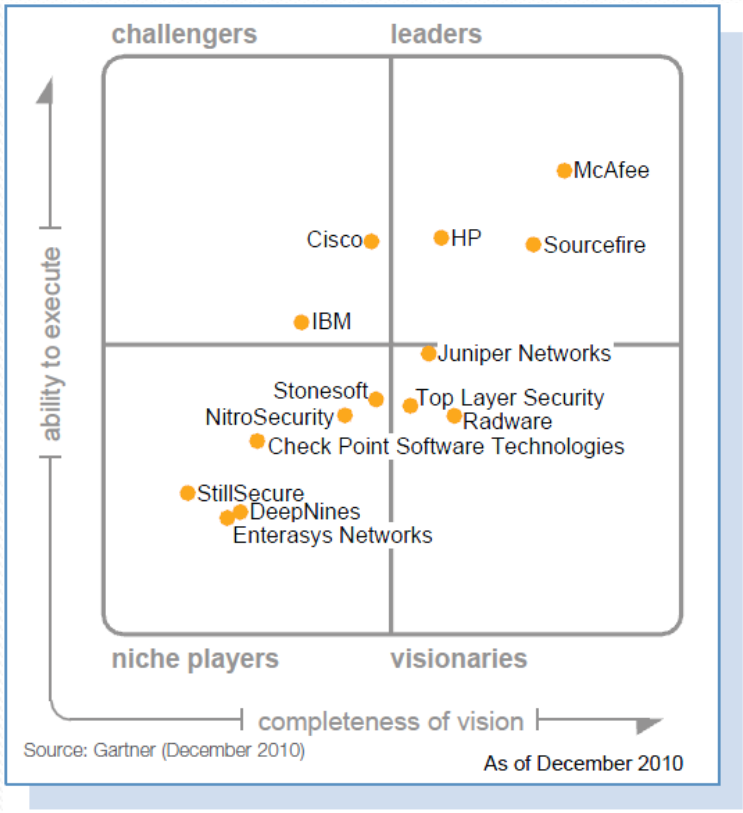
- Más sobre multi-threading

  - Adquisición de paquetes
  - Decodificación
  - Capa de flujo de datos
  - Detecciones y salidas



Descripción y Estado actual del IDS/IPS Suricata

- Comparación con otras soluciones IDS/IPS
  - Soluciones propietarias
    - McAffee
    - CISCO
    - Tipping Point
    - SourceFire



Descripción y Estado actual del IDS/IPS Suricata

- Comparación con otras soluciones IDS/IPS
  - Soluciones Propietarias

Características	Soluciones Comerciales IDS/IPS	Suricata
Multi-Threading	x	Si
Soporte para IPV6	Cisco, IBM, Stonesoft	Si
IP Reputation	Cisco	Si
Detección Autamática de Protocolos	No	Si
Aceleración con GPU	No	Si
Variables Globales/Flowbit	No	Si
GeoIP	No	Si
Análisis Avanzado de HTTP	No	Si
HTTP Access Logging	No	Si
SMB Access Logging	No	Si
Anomaly Detection	Sí	No
Alta Disponibilidad	Si	No
GUI de Administración	Si	No
GRATIS	No	SI

Tabla 2.1 Comparación de Suricata con IPS/IDS's propietarias

Descripción y Estado actual del IDS/IPS Suricata

- Soluciones Open Source
  - Bro y Snort

Características	Bro	Snort	Suricata
Multi-Threading	No	x	Si
Soporte para IPV6	Si	Sí	Si
IP Reputation	Algo	No	Si
Detección Autamática de Protocolos	Si	No	Si
Aceleración con GPU	No	No	Si
Variables Globales/Flowbits	Si	No	Si
GeoIP	Si	No	Si
Análisis Avanzado de HTTP	Si	No	Si
HTTP Access Logging	Si	No	Si
SMB Access Logging	Si	No	Si

Tabla 2.2 Comparación de Suricata con IPS/IDS's de código abierto

Descripción y Estado actual del IDS/IPS Suricata

- Fortalezas
  - Primer IPS/IDS que utiliza tecnología multi-hilos
  - Permite que otras herramientas sean compatibles con el sistema
- Oportunidades
  - Da paso a mejoras sustanciales de detección de intrusos
  - Pymes pueden aprovechar el bajo costo de implementación de una solución Software Libre.

Descripción y Estado actual del IDS/IPS Suricata

- Debilidades
  - Herramienta muy joven en procesos de mejoras y optimización.
  - Desconfianza en aquellos que no creen en el Software Libre.
  - Dependencia de desarrollos externos.
- Amenazas
  - Nuevas soluciones usando el mismo código que es Shareware.
  - Nuevos ataques no sean rápidamente solucionables.

Descripción y Estado actual del IDS/IPS Suricata

- Futuras mejoras de Suricata
  - Aceleración con CUDA/GPU
  - Reputación IP y DNS
  - Salidas por medio de sockets
  - Preprocesador de anomalías
  - Actualización de módulos sin reiniciar todo Suricata.
  - Más información de estadísticas de detección.

Agenda

- Antecedentes y Objetivos
- Descripción del Estado Actual del IDS/IPS Suricata
- Diseño e implementación de la solución IDS/IPS Empresarial
- Diseño e integración del módulo de detección de anomalías
- Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías
- Propuestas de mejoras para la solución empresarial actual
- Conclusiones y recomendaciones

Diseño e implementación de la solución IDS/IPS Empresarial

- Configuración de Suricata
- Reglas para la detección de ataques.
- Módulo Colector de Alertas
- Módulo de Recuperación de Fallos
- Interfaz de Administración
- Módulo para Detección de Anomalías

Diseño e implementación de la solución IDS/IPS Empresarial

- **Configuración de Suricata**
  - Max pending packets

```
# Number of packets allowed to be processed simultaneously.  Default is a
# conservative 50. a higher number will make sure CPU's/CPU cores will be
# more easily kept busy, but will negatively impact caching.

max-pending-packets: 400
```

Diseño e implementación de la solución IDS/IPS Empresarial

- **Configuración de Suricata**
  - Salidas de Alertas y Registros

```
# Configure the type of alert (and other) logging you would like.
outputs:

  # a line based alerts log similar to Snort's fast.log
  - fast:
      enabled: yes
      filename: fast.log
```

```
# alert output for use with Barnyard2
- unified2-alert:
    enabled: yes
    filename: unified2.alert

    # Limit in MB.
    #limit: 32
```

Diseño e implementación de la solución IDS/IPS Empresarial

- **Configuración de Suricata**
  - Multithreading

```
set_cpu_affinity: yes

# Tune cpu affinity of suricata threads. Each family of threads can be bound
#??on specific CPUs.
cpu_affinity:
  - management_cpu_set:
      cpu: [ 0 ]  # include only these cpus in affinity settings
  - receive_cpu_set:
      cpu: [ "4-7" ]  # include only these cpus in affinity settings
      mode: "exclusive"
      prio:
       default:"high"
  - decode_cpu_set:
      cpu: [ 0, 1 ]
      mode: "balanced"
  - stream_cpu_set:
      cpu: [ "0-1" ]
  - detect_cpu_set:
      cpu: [ "0-3" ]
      mode: "exclusive" # run detect threads in these cpus
      prio:
```

Diseño e implementación de la solución IDS/IPS Empresarial

- **Configuración de Suricata**
  - Variables de red local

```
# Holds variables that would be used by the engine.
vars:

  # Holds the address group vars that would be passed in a Signature.
  # These would be retrieved during the Signature address parsing stage.
  address-groups:

    HOME_NET: 192.168.0.0/16,10.0.0.0/8,172.16.0.0/12

    EXTERNAL_NET: any

    HTTP_SERVERS: $HOME_NET

    SMTP_SERVERS: $HOME_NET

    SQL_SERVERS: any

    DNS_SERVERS: $HOME_NET

    TELNET_SERVERS: $HOME_NET
```

Diseño e implementación de la solución IDS/IPS Empresarial

- **Configuración de Suricata**
  - Reglas a cargar

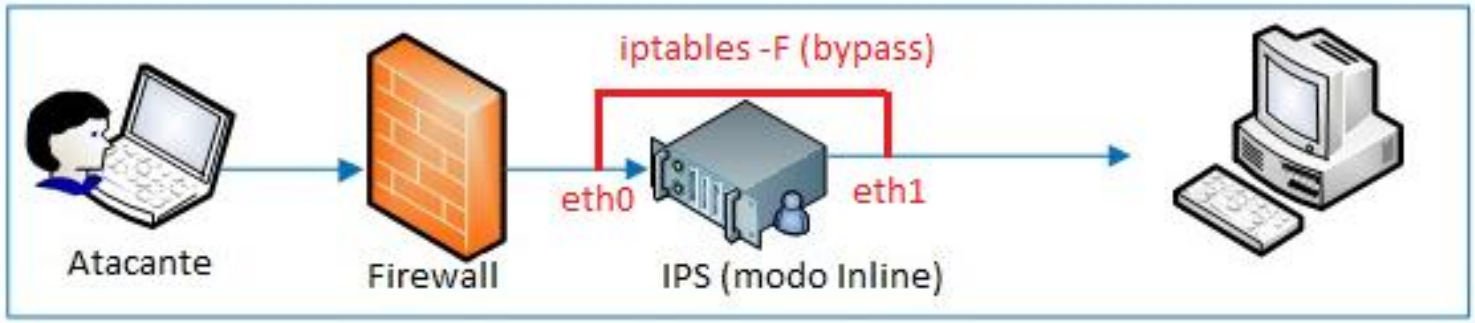
```
rule-files:
 - emerging-ftp.rules
 - emerging-policy.rules
 - emerging-trojan.rules
 - emerging-games.rules
 - emerging-pop3.rules
 - emerging-user_agents.rules
 - emerging-activex.rules
 - emerging-rpc.rules
 - emerging-virus.rules
 - emerging-attack_response.rules
 - emerging-icmp.rules
 - emerging-scan.rules
 - emerging-voip.rules
 - emerging-chat.rules
 - emerging-icmp_info.rules
 - emerging-shellcode.rules
 - emerging-web_client.rules
```

Diseño e implementación de la solución IDS/IPS Empresarial

- **Reglas y firmas de seguridad**
  - Suricata depende de reglas externas para su funcionamiento.
  - Desarrolladores conocidos: **Emerging Threats** y Sourcefire
  - Sets de reglas gratuitas y pagadas.
  - Tiempo de actualización.
  - **Oinkmaster** para actualización de reglas.

Diseño e implementación de la solución IDS/IPS Empresarial

- **Módulo de recuperación de fallos**
  - Modo Inline, interfaces en modo Bridge.
  - Flush de reglas de iptables.
  - Script de Recuperación de Fallos



Diseño e implementación de la solución IDS/IPS Empresarial

- **Módulo de recuperación de fallos**

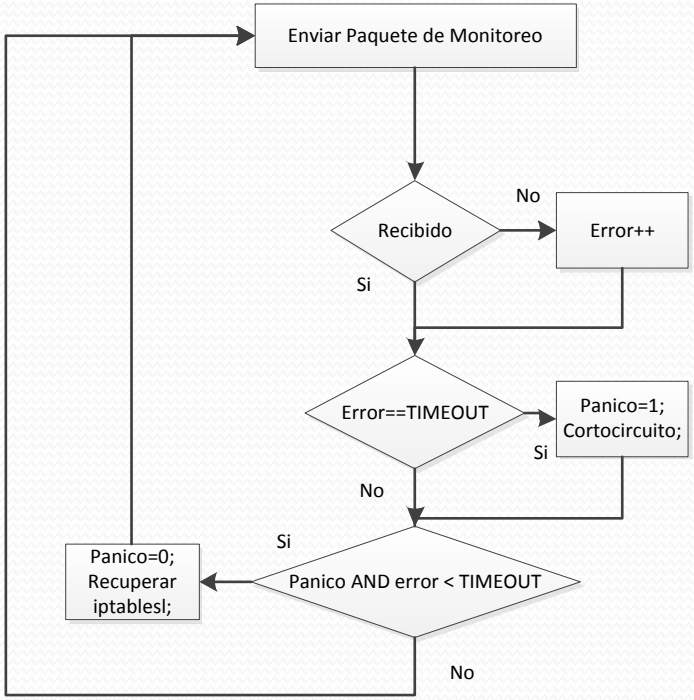


Figura 3.15 Diagrama de estados del módulo de recuperación de fallos

Diseño e implementación de la solución IDS/IPS Empresarial

- **Módulo colector de alertas**
  - Barnyard2
  - Recoge los archivos de salida estándar unified2.
  - Se guarda los eventos en una base de datos

- **Instalador de la solución empresarial**
  - Paquete RPM

Diseño e implementación de la solución IDS/IPS Empresarial

- Diseño de la interfaz gráfica de administración
  - CodeIgniter
  - MVC

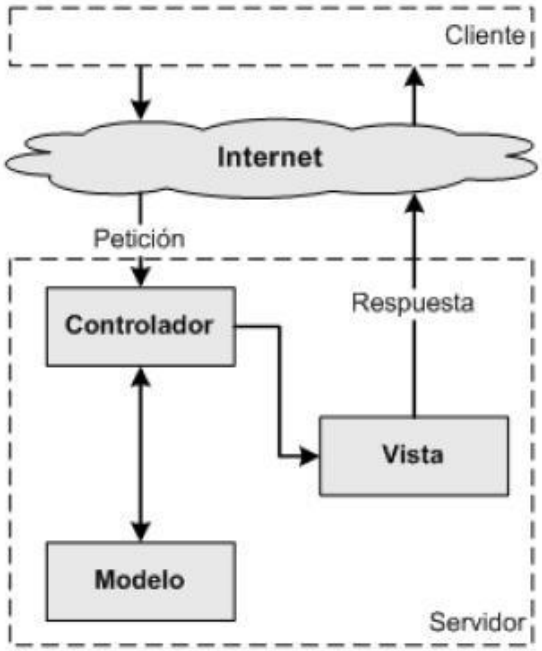


Figura 3.1: Diagrama de Arquitectura MVC.

Diseño e implementación de la solución IDS/IPS Empresarial

- MVC

Estructura MVC de la Interfaz		
Controladores	**Modelos**	**Vistas**
• general • herramientas • inicio • principal • reportes • ruleset • suricata	• general_model • modulo_model • reportes_model • ruleset_model • suricata_model	• consultar_reportes • general • menu_principal • phpterm • reportes • ruleset • ruleset_consultar • ruleset_consultar_todo • suricata

Diseño e implementación de la solución IDS/IPS Empresarial

- Módulos de operación de la interfaz

Agenda

- Antecedentes y Objetivos
- Descripción del Estado Actual del IDS/IPS Suricata
- Diseño e implementación de la solución IDS/IPS Empresarial
- Diseño e integración del módulo de detección de anomalías
- Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías
- Propuestas de mejoras para la solución empresarial actual
- Conclusiones y recomendaciones

Diseño e integración del módulo de detección de anomalías

- Antecedentes
  - Denning lo introdujo.
  - Axelsson: Se considera detección de anomalías como auto aprendizaje
  - Módulo de detección de anomalías de por sí detecta mas no alerta.

Diseño e integración del módulo de detección de anomalías

- Herramienta Ourmon
  - Sistema de detección de anomalías desarrollado por James Binkley.
  - BPF, RRDTOOL
  - Monitorear flujos TCP y UDP
  - Atrapa servidores de correo en modo relay
  - Atrapa botnets
  - Observa que protocolos están utilizando el mayor ancho de banda

Diseño e integración del módulo de detección de anomalías

- Algoritmos de detección de anomalías usado por Ourmon
  - Tráfico TCP
    - Tuplas SYN
      - *(IP Source address, SYNS, SYNACKS, FINSSENT, FINSBACK, RESETS, ICMP ERRORS, PKTSSENT, PKTSBACK, port signature data)*
    - Pesos asociados a la tupla SYN: Work Weight y Worm Weight

$$(S_S + F_s + R_r)/T_{sr}$$

Work Weight

$$S_s - F_r > C$$

Worm Weight

Diseño e integración del módulo de detección de anomalías

- Tráfico TCP

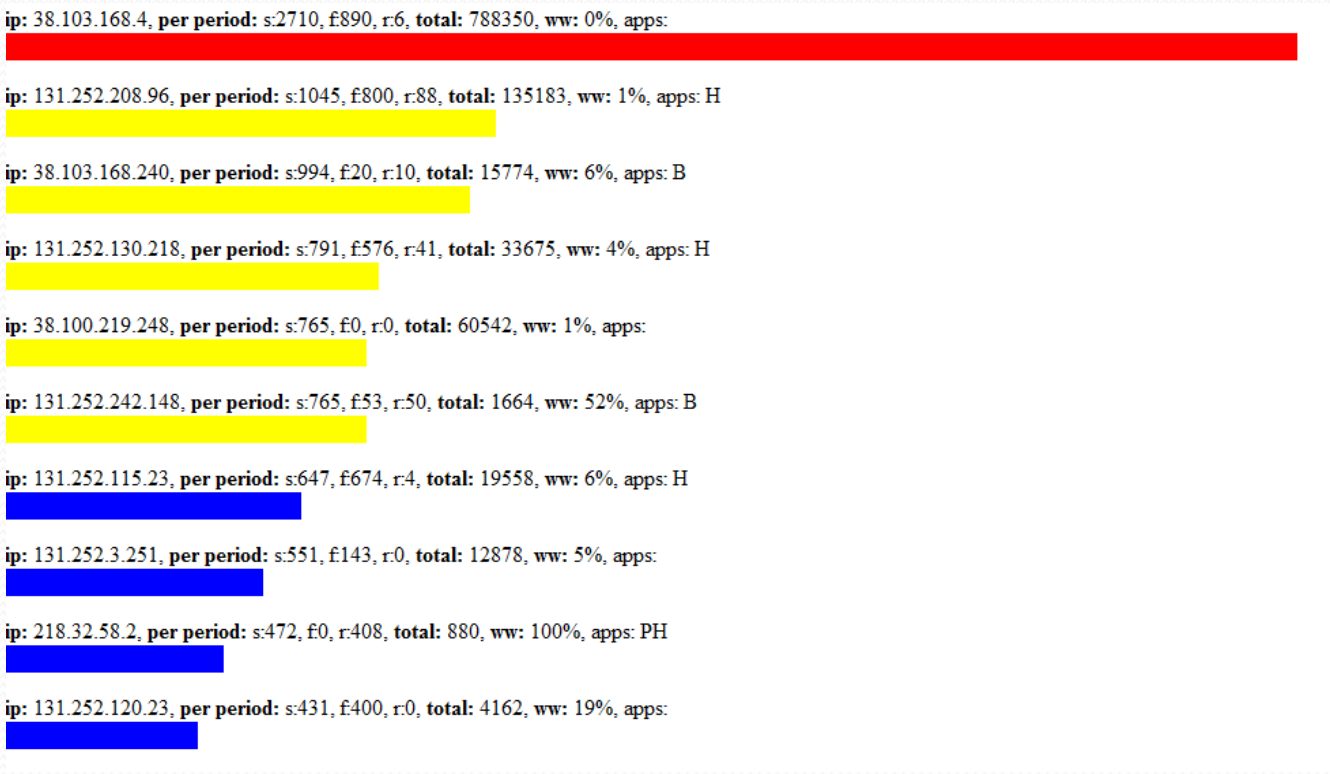


Figura 4.2: Lista de IPs que entran al campus.

Diseño e integración del módulo de detección de anomalías

- Tráfico TCP

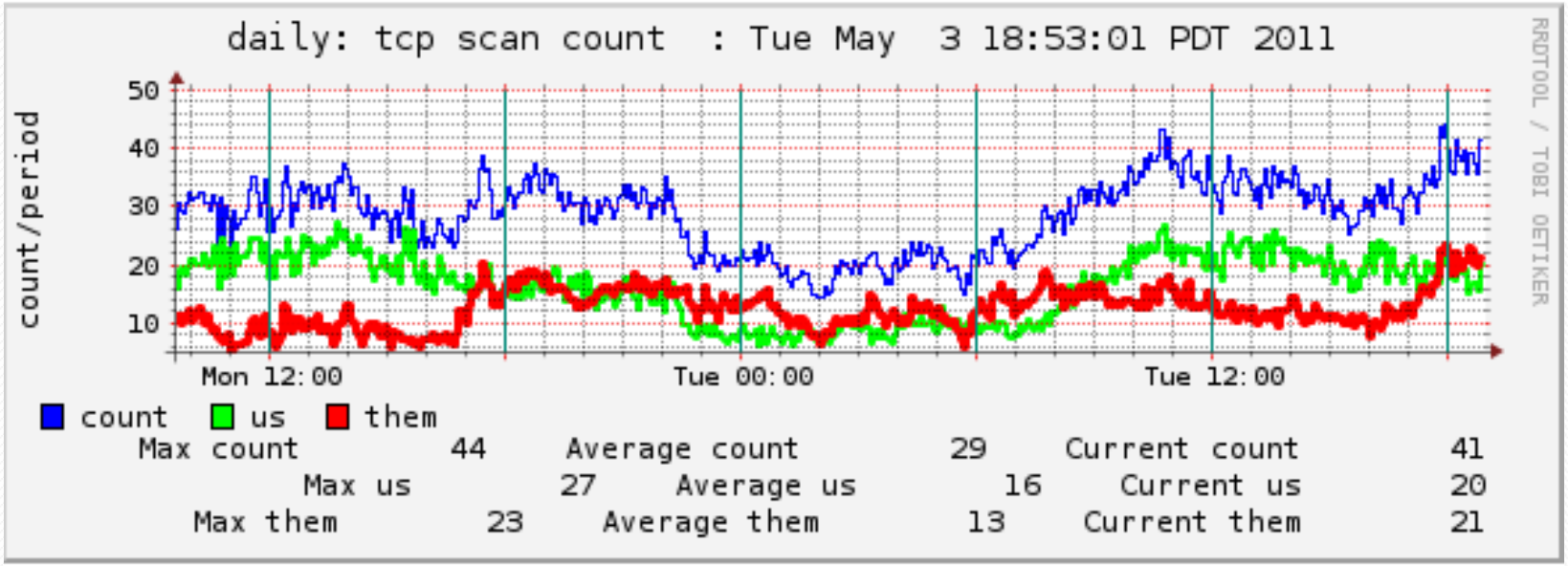


Figura 4.3 Grafo de detección de gusanos utilizando Ourmon.

Diseño e integración del módulo de detección de anomalías

- Tráfico UDP
  - Tuplas UDP
    - *(IPSRC, WEIGHT, SENT, RECV, ICMPERRORS, L3D, L4D, SIZEINFO, SA/RA, APPFLAGS, PORTSIG).*

*Peso de trabajo = (SENT * ICMPERRORS) + REC*

Diseño e integración del módulo de detección de anomalías

- Tráfico UDP

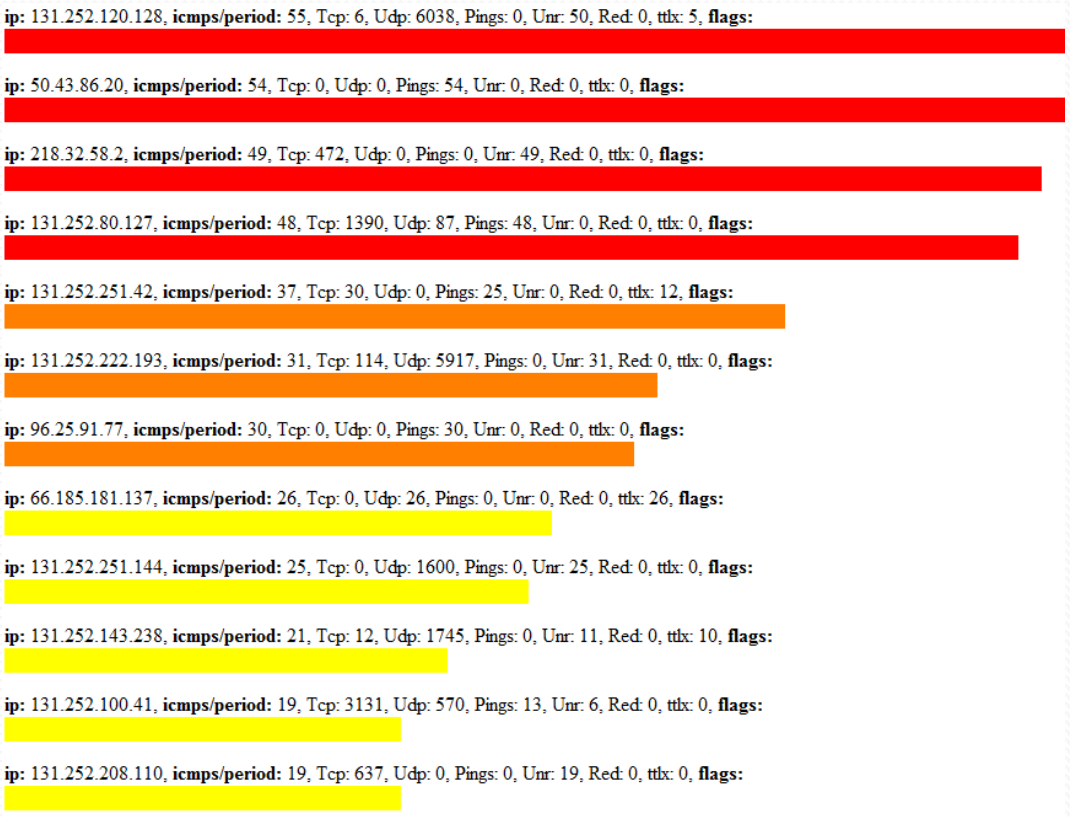


Figura 4.5 Lista con las IPs y sus respectivos ICMP Errors.

Diseño e integración del módulo de detección de anomalías

- Integración final de la solución IDS/IPS Empresarial
  - Tcpworm.txt
  - Script realiza lecturas del archivo cada minuto accediendo a la información IP sospechosa
  - Ourmon-anomaly.rules

```
alert ip -SUSPICIOUS_IP- any -> $HOME_NET any (
msg:"Anomaly Detected, possible worm attack";
classtype: anomaly-ourmon; sid:1100000; rev:1;)
```

Figura 4.6 Regla generada para alertar el host sospechoso detectado por ourmon

Diseño e integración del módulo de detección de anomalías

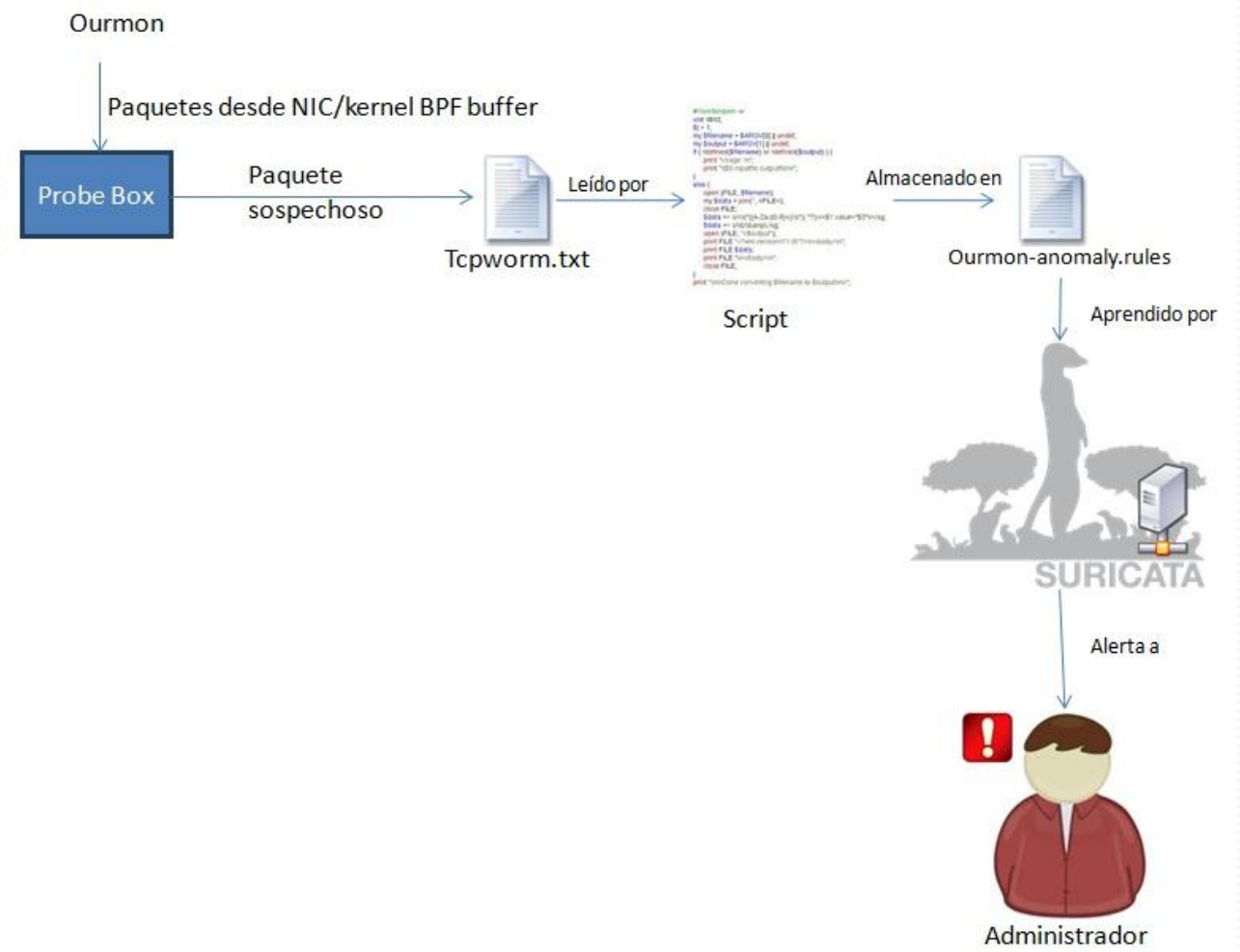


Figura 4.7: Diagrama de módulo de detección de anomalías y auto aprendizaje

Agenda

- Antecedentes y Objetivos
- Descripción del Estado Actual del IDS/IPS Suricata
- Diseño e implementación de la solución IDS/IPS Empresarial
- Diseño e integración del módulo de detección de anomalías
- Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías
- Propuestas de mejoras para la solución empresarial actual
- Conclusiones y recomendaciones

Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías

- Hardware usado para las pruebas
  - Motherboard: Intel Corporation DP55WB
  - Procesador: Intel(R) Core(TM) i7 CPU 870@2.93GHz
  - Memoria RAM: 8 Gigas
  - Tarjetas de Red: 3 Intel 82572EI Gigabit Ethernet
- Software utilizado para las pruebas
  - Tomahawk
  - Hping3
  - iperf
  - Httperf
  - Siege

Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías

- Escenario y topología para las pruebas

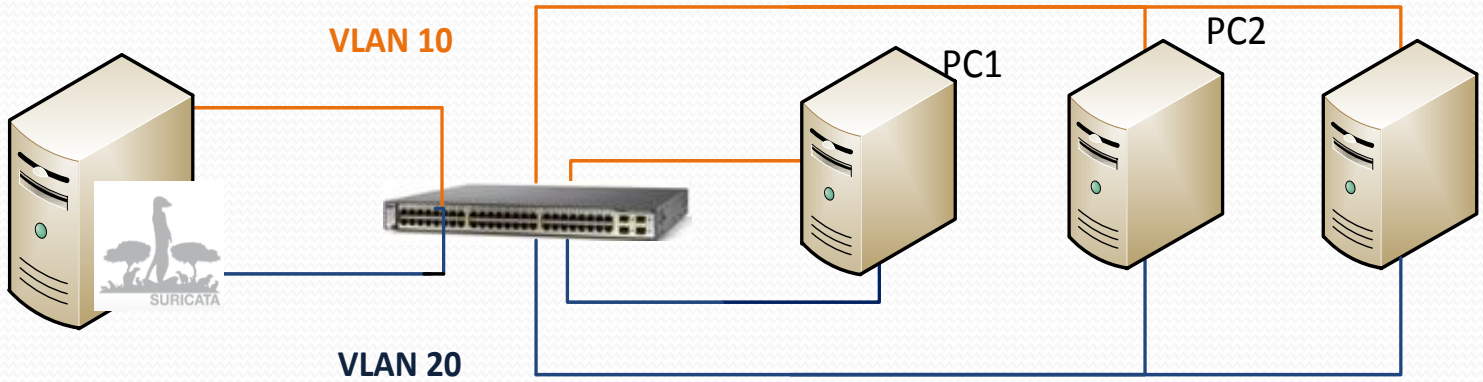


Figura 5.1 Topología para las pruebas

Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías

- Prueba 1: CPU vs Throughput en modo IDS

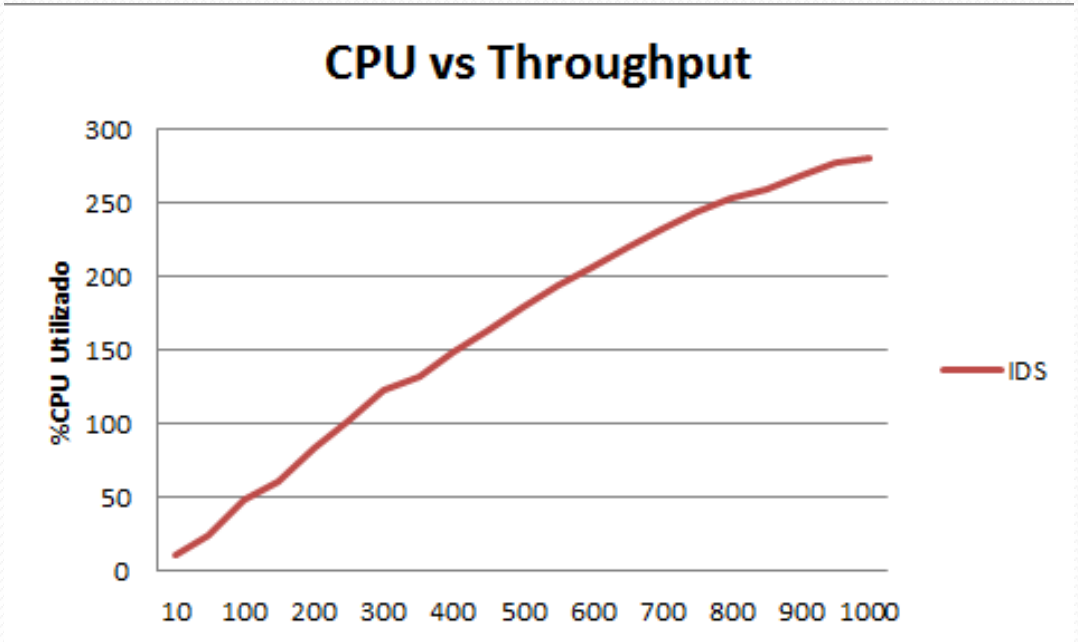


Figura 5.2: Utilización de CPU vs Througput en modo IDS

Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías

- Prueba 2: CPU vs Throughput en modo IPS

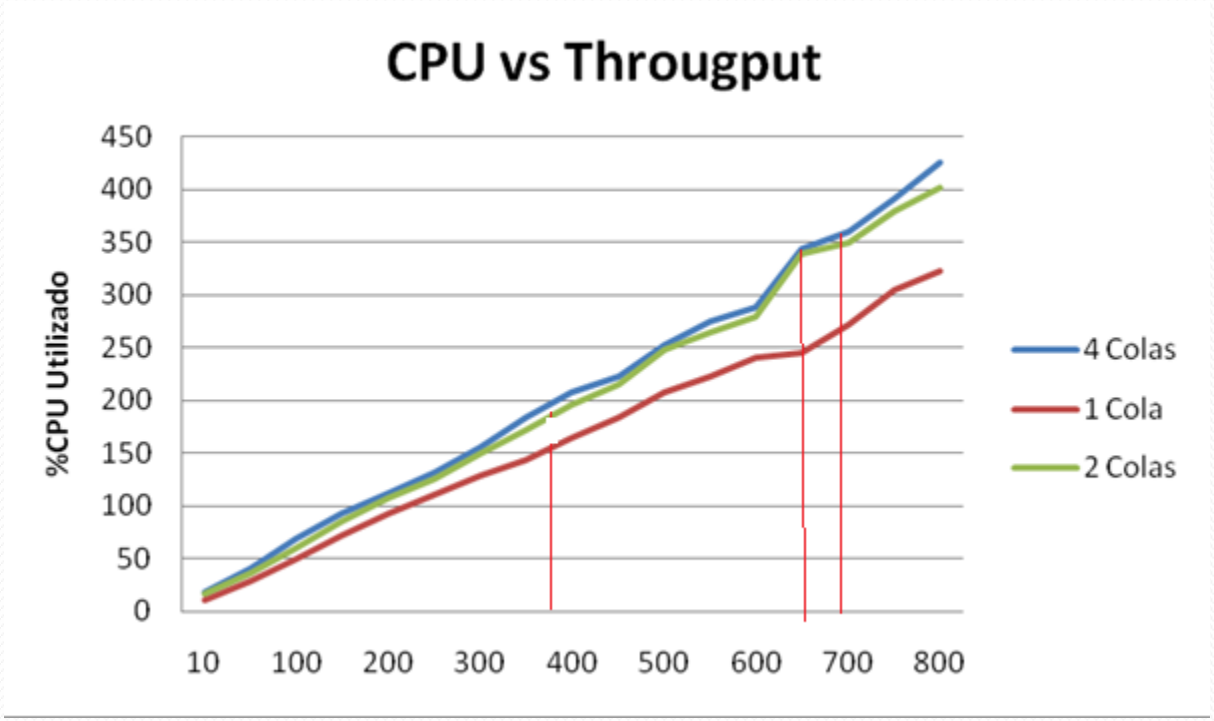


Figura 5.3: Utilización de CPU vs Througput en modo IPS

Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías

TGID	TID	%usr	%system	%guest	%CPU	CPU	Command
21634	-	169.00	146.00	0.00	315.00	1	suricata
-	21634	0.00	0.00	0.00	0.00	1	|__suricata
-	21641	3.00	7.00	0.00	10.00	5	|__RecvNFQ-Q1
-	21642	2.00	6.00	0.00	8.00	6	|__RecvNFQ-Q2
-	21643	7.00	1.00	0.00	8.00	7	|__RecvNFQ-Q3
-	21644	3.00	7.00	0.00	10.00	4	|__RecvNFQ-Q4
-	21645	15.00	13.00	0.00	28.00	1	|__Decode1
-	21646	7.00	2.00	0.00	9.00	0	|__Detect1
-	21647	5.00	4.00	0.00	9.00	2	|__Detect2
-	21648	8.00	2.00	0.00	10.00	1	|__Detect3
-	21649	10.00	0.00	0.00	10.00	3	|__Detect4
-	21650	8.00	2.00	0.00	10.00	0	|__Detect5
-	21651	11.00	0.00	0.00	11.00	1	|__Detect6
-	21652	7.00	2.00	0.00	9.00	2	|__Detect7
-	21653	5.00	4.00	0.00	9.00	3	|__Detect8
-	21654	7.00	3.00	0.00	10.00	0	|__Detect9
-	21655	7.00	3.00	0.00	10.00	1	|__Detect10
-	21656	9.00	1.00	0.00	10.00	2	|__Detect11
-	21657	10.00	0.00	0.00	10.00	3	|__Detect12
-	21658	10.00	0.00	0.00	10.00	0	|__Detect13
-	21659	10.00	1.00	0.00	11.00	1	|__Detect14
-	21660	6.00	4.00	0.00	10.00	2	|__Detect15
-	21661	5.00	4.00	0.00	9.00	3	|__Detect16
-	21662	2.00	15.00	0.00	17.00	4	|__VerdictNFQ0
-	21663	3.00	19.00	0.00	22.00	5	|__VerdictNFQ1
-	21664	4.00	18.00	0.00	22.00	6	|__VerdictNFQ2
-	21665	2.00	20.00	0.00	22.00	7	|__VerdictNFQ3
-	21666	4.00	4.00	0.00	8.00	3	|__Outputs
-	21667	4.00	2.00	0.00	6.00	4	|__FlowManagerThre
-	21668	0.00	0.00	0.00	0.00	2	|__SCPerfWakeupThr
-	21669	0.00	0.00	0.00	0.00	4	|__SCPerfMgmtThrea

Figura 5.4 Procesamiento de Suricata por Hilos con 4 colas

Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías

```
Tasks: 148 total,   1 running, 147 sleeping,   0 stopped,   0 zombie
Cpu0  :  9.8%us, 23.4%sy, 36.6%ni, 30.2%id,  0.0%wa,  0.0%hi,  0.0%si,
Cpu1  : 43.9%us, 18.0%sy,  0.0%ni, 38.0%id,  0.0%wa,  0.0%hi,  0.0%si,
Cpu2  : 36.1%us,  6.5%sy,  0.0%ni, 57.4%id,  0.0%wa,  0.0%hi,  0.0%si,
Cpu3  : 35.5%us,  4.7%sy,  0.0%ni, 59.9%id,  0.0%wa,  0.0%hi,  0.0%si,
Cpu4  :  4.3%us, 13.7%sy,  0.0%ni, 61.2%id,  0.0%wa,  0.0%hi, 20.7%si,
Cpu5  :  6.4%us, 10.6%sy,  0.0%ni, 61.4%id,  0.0%wa,  0.0%hi, 21.5%si,
Cpu6  :  9.7%us, 19.1%sy,  0.0%ni, 67.7%id,  0.0%wa,  0.0%hi,  3.5%si,
Cpu7  : 11.0%us, 20.7%sy,  0.0%ni, 64.9%id,  0.0%wa,  0.0%hi,  3.4%si,
Mem:   8174536k total,  2340340k used,  5834196k free,   133192k buffers
Swap:  1052248k total,        0k used,  1052248k free,   770272k cached

21634 root      20   0 1607m 1.1g 1732 S  338 13.8  37:26.52 suricata
   33 root      20   0     0    0    0 S    0  0.0   6:43.84 events/6
    1 root      20   0  3852  668  568 S    0  0.0   0:03.30 init
  867 root      20   0     0    0    0 S    0  0.0   0:04.82 kjournald
```

Figura 5.5 Procesamiento de Suricata por procesador con 4 colas

Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías

- Pruebas del módulo de detección de anomalías

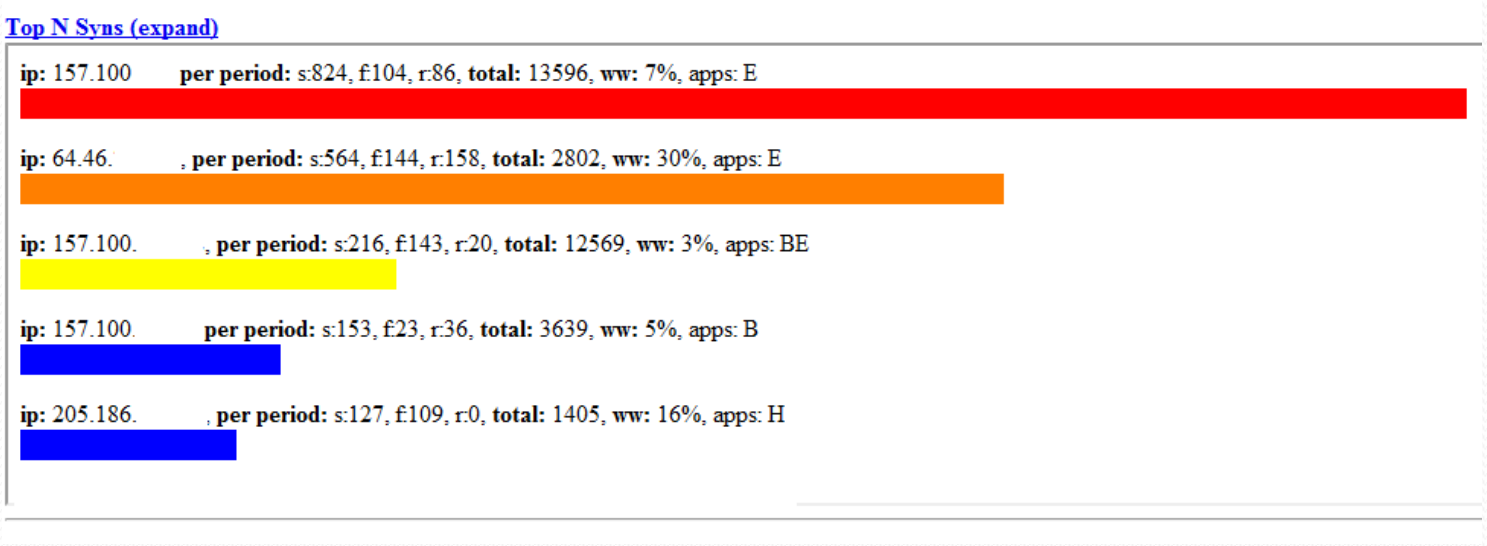


Figura 5.6: Top Syns que entran a la red.

Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías

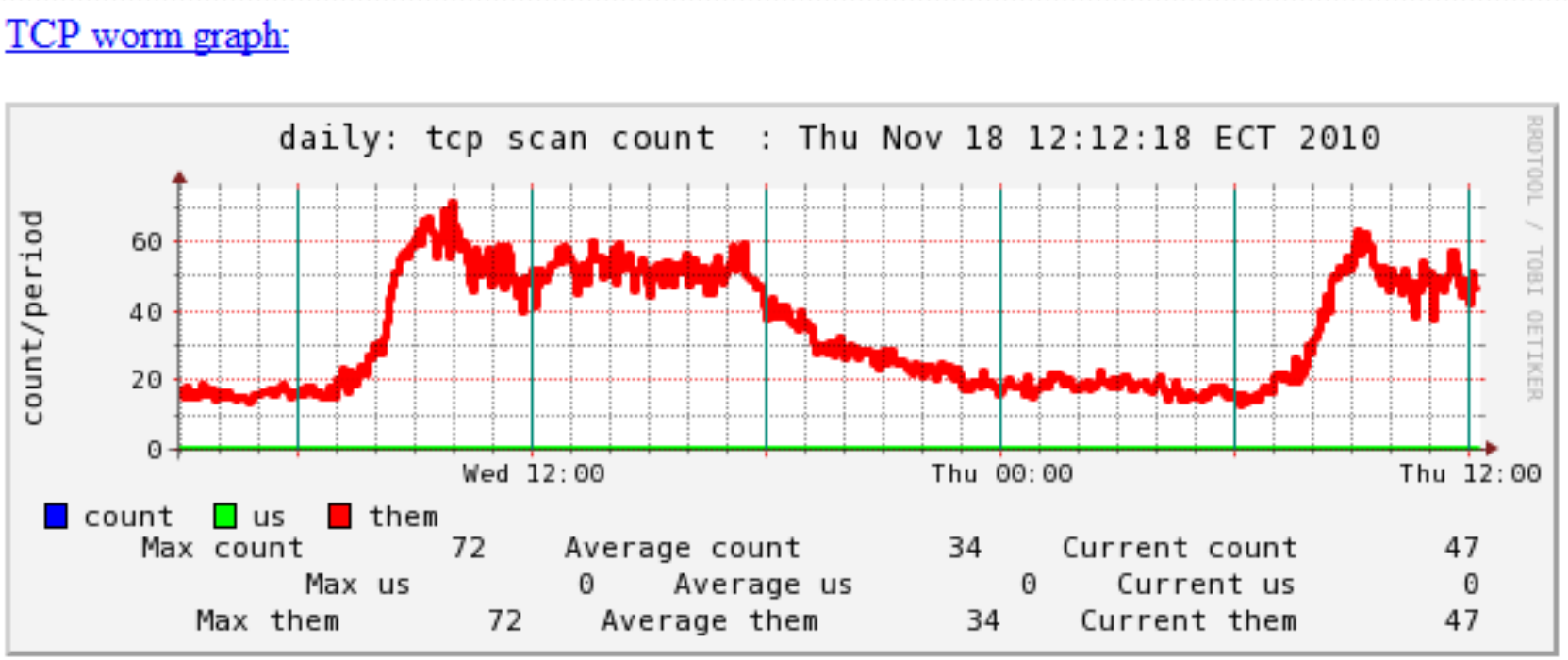


Figura 5.7 Grafo de detección de gusanos utilizando Ourmon.

Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías

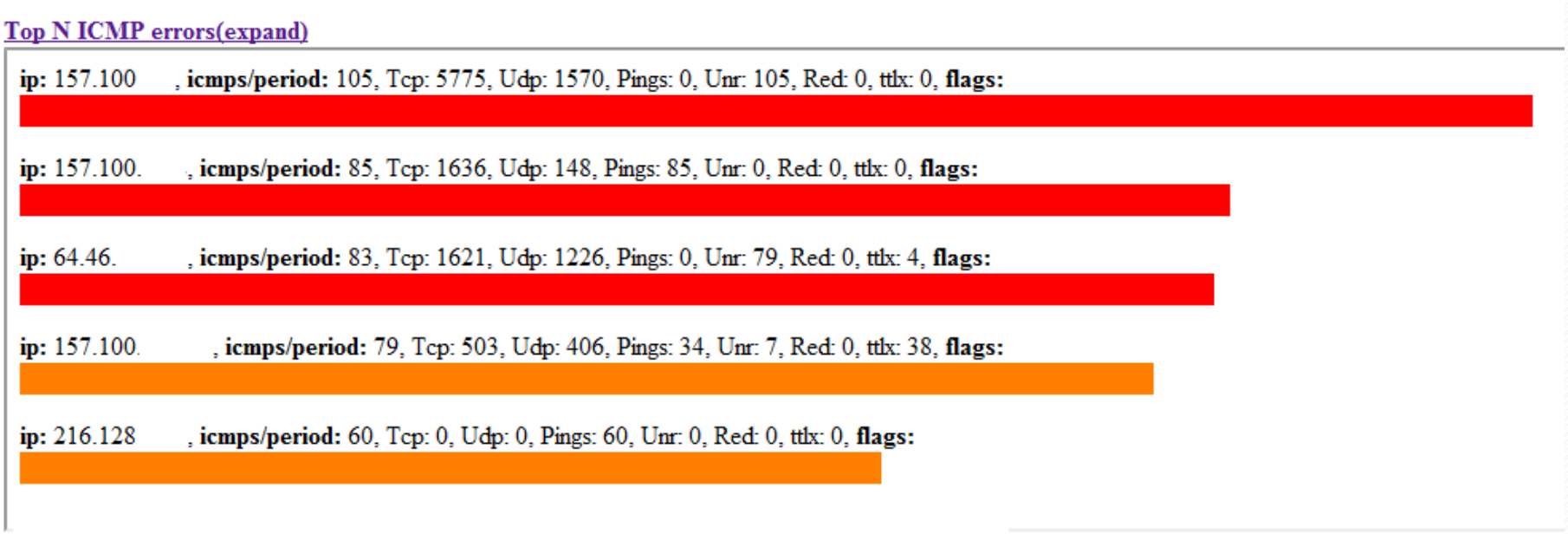


Figura 5.8 Lista con las IPs y sus respectivos ICMP Errors.

Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías

```
top - 23:23:18 up 15 days,  6:36,  3 users,  load average: 0.21, 0.14, 0.10
Tasks: 168 total,   1 running, 167 sleeping,   0 stopped,   0 zombie
Cpu(s):  1.6%us,  0.1%sy,  0.0%ni, 98.3%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   8301656k total,  2766700k used,  5534956k free,   310040k buffers
Swap:  5406716k total,        0k used,  5406716k free,  1835844k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 2657 root      20   0  2020  448  372 S  0.3  0.0   9:38.22 hald-addon-stor
 2819 mysql     20   0 2082m 356m 5560 S  0.3  4.4  51:42.87 mysqld
11449 root      20   0 13920  11m  880 S  0.3  0.1   0:03.09 ourmon
15553 root      20   0  2380  964  704 S  0.3  0.0   0:02.71 top
    1 root      20   0  2116  596  504 S  0.0  0.0   0:07.71 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
```

Figura 5.11 Rendimiento de procesador y memoria de Ourmon

Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías

- Conclusiones de las pruebas y resultados
  - Redes Gigabit ethernet empieza a limitar el throughput
  - A pesar del limitante del throughput, el procesador no estuvo saturado
  - Correr Suricata a altas velocidades sin optimizar disminuye el desempeño del motor
  - Incremento de desempeño = mayor memoria RAM
  - Suricata aprendió del módulo de detección de anomalías

Agenda

- Antecedentes y Objetivos
- Descripción del Estado Actual del IDS/IPS Suricata
- Diseño e implementación de la solución IDS/IPS Empresarial
- Diseño e integración del módulo de detección de anomalías
- Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías
- Propuestas de mejoras para la solución empresarial actual
- Conclusiones y recomendaciones

Propuestas de mejoras para la solución empresarial actual

- Interfaz gráfica de gestión y control remoto

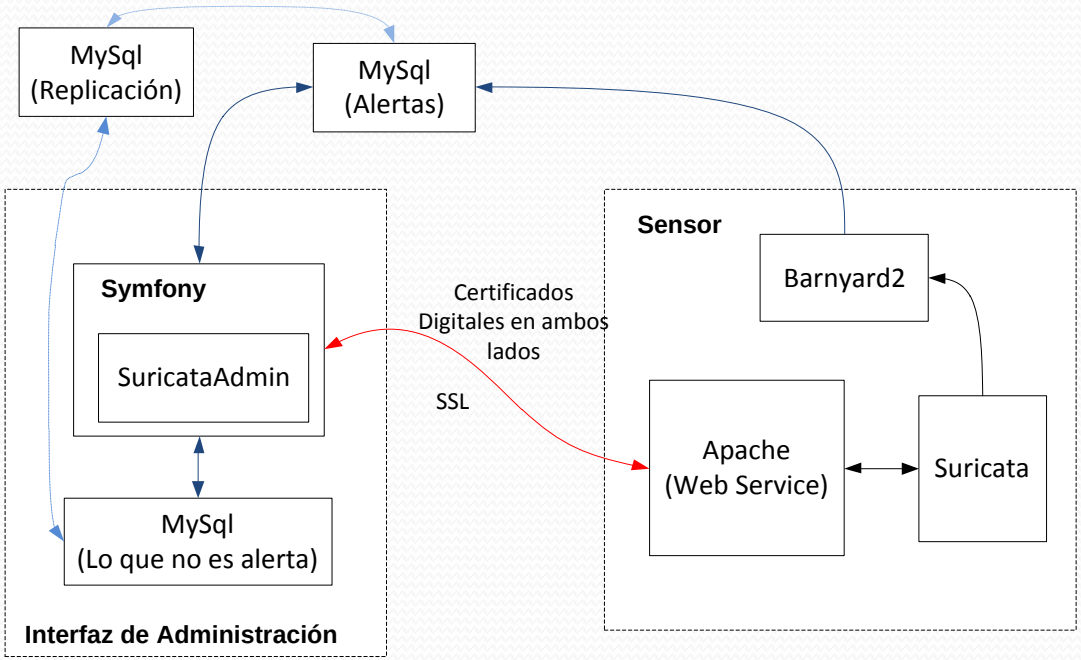


Figura 6.1: Diagrama de bloques para una interfaz centralizada

Propuestas de mejoras para la solución empresarial actual

- Interfaz gráfica de gestión y control remoto

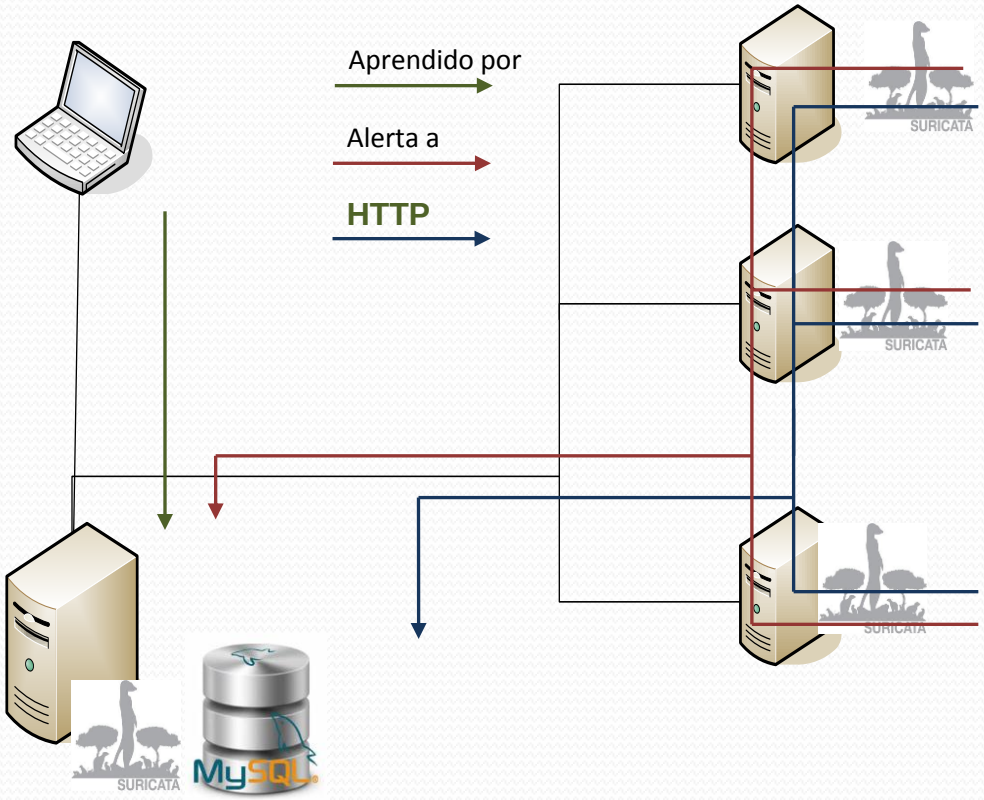


Figura 6.2: Diagrama Web Service para una interfaz centralizada

Propuestas de mejoras para la solución empresarial actual

- Módulo de monitoreo para Centro de Operaciones de Redes
- Módulo de detección reactiva de Suricata en modo IDS
- Otras propuestas de mejoras
  - Integración del módulo de detección de anomalías al motor
  - Integración del módulo de recuperación de fallos y alta Disponibilidad al motor
  - Análisis y optimización del código para aumentar el throughput máximo.

Agenda

- Antecedentes y Objetivos
- Descripción del Estado Actual del IDS/IPS Suricata
- Diseño e implementación de la solución IDS/IPS Empresarial
- Diseño e integración del módulo de detección de anomalías
- Diseño y ejecución de pruebas de rendimiento de Suricata y del Módulo de detección de anomalías
- Propuestas de mejoras para la solución empresarial actual
- Conclusiones y recomendaciones

Conclusiones y Recomendaciones

- Conclusiones
  - Los IDS/IPS son herramientas necesarias para tener una protección completa de cualquier arquitectura computacional en los negocios.
  - Todas las herramientas utilizadas en esta tesina de seminario de grado han sido de código abierto, demostrando la compatibilidad entre ellas y consistencia durante el desarrollo de esta tesina de seminario.
  - Se estableció patrones de medición de rendimiento utilizando libcaps de tráfico pesado para evaluar la capacidad de Suricata de analizar dicho tráfico sacando provecho la tecnología multi-hilos que lo caracteriza.

Conclusiones y Recomendaciones

- Recomendaciones
  - Es necesario definir políticas y procedimientos de seguridad dentro de la empresa.
  - Capacitar al personal encargado del mantenimiento de la solución.
  - Mantener actualizada las reglas de ET.
  - Concientizar a empresarios acerca de la Seguridad Informática