Curso Superior de Tecnologia em Redes de Computadores
Projeto Integrador

Projeto Integrador

Gabriel Jesus Pereira
gabroot.pereira@gmail.com.br

SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL
FACULDADE DE TECNOLOGIA SENAC PELOTAS

Análise dos Sistemas de **IDS/IPS** em Redes

&

Gabriel Jesus Pereira

Sumário

Introdução

- Motivação / Justificativa

  - Confidencialidade
  - Integridade
  - Disponibilidade

Objetivos

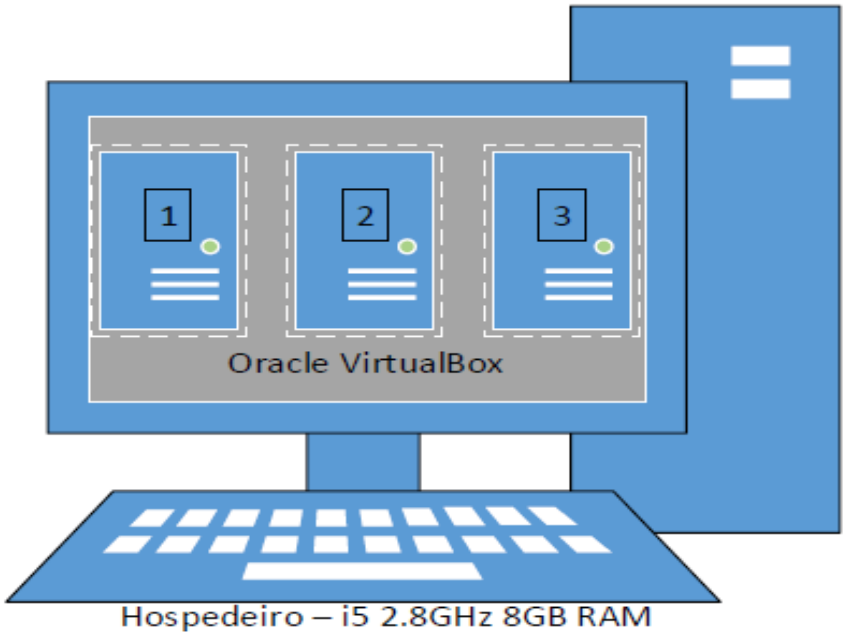
- Objetivo Geral:
  - Realizar um estudo analítico e comparativo entre dois sistemas de detecção e prevenção de intrusão para verificar qual pode ser mais assertivo.

- Objetivos Específicos:
  - Pesquisa;
  - Cenário de testes;
  - Realização de testes;
  - Comparação de resultados;

Metodologia

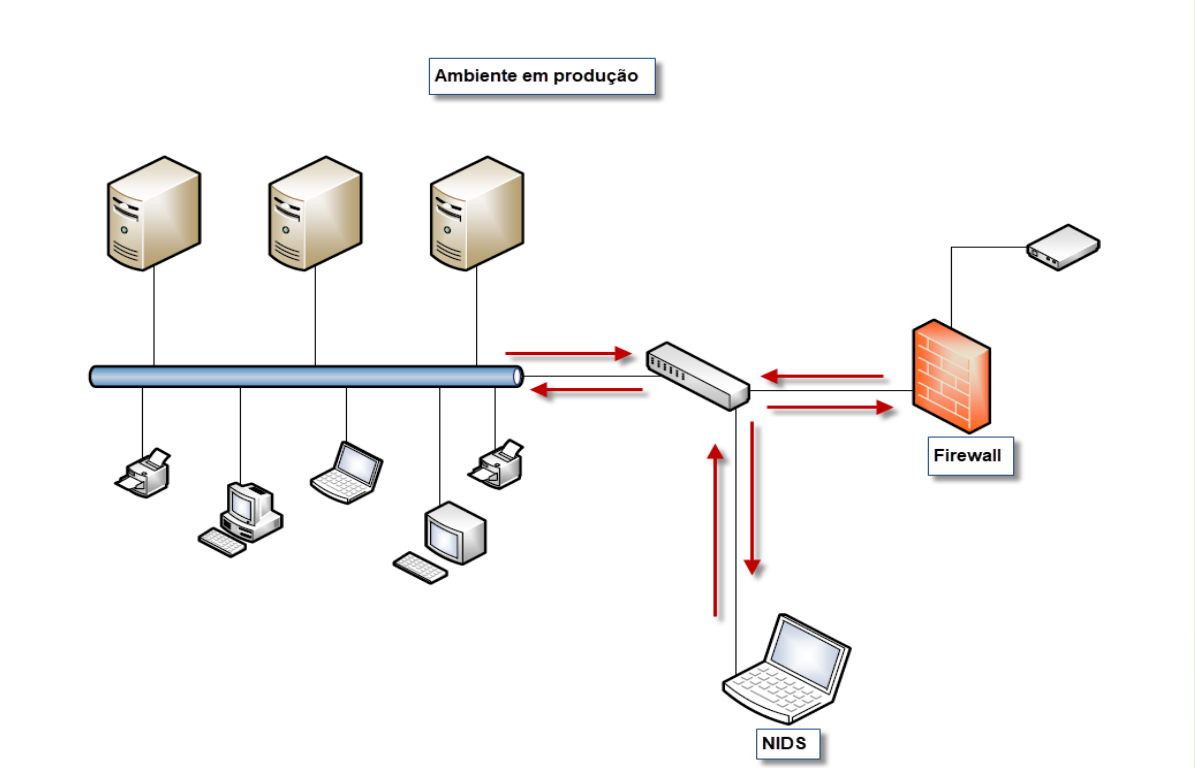
- Ambiente virtualizado
- Ambiente em produção

Ambiente Virtualizado



Máquina 1 - Ubuntu Server 14.4 - Snort 2.9.9
Máquina 2 - Ubuntu Server 14.4 - Suricata 3.2.1
Máquina 3 - Kali Linux

Ambiente em produção



Resultados – Ambiente Virtualizado

Snort – *Brute Force*

Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
2	Snort	192.168.201.145	192.168.201.202	ET SCAN Potential SSH Scan OUTBOUND	11:04 PM
2	Snort	192.168.201.145	192.168.201.202	GPL SCAN nmap fingerprint attempt	11:04 PM
3	Snort	192.168.201.202	192.168.201.145	GPL ICMP Echo Reply undefined code	11:04 PM
3	Snort	192.168.201.145	192.168.201.202	GPL ICMP_INFO PING	11:04 PM
3	Snort	192.168.201.202	192.168.201.145	GPL ICMP_INFO Echo Reply	11:04 PM
1	Snort	192.168.201.145	192.168.201.202	GPL SHELLCODE x86 inc ebx NOOP	11:04 PM
2	Snort	192.168.201.145	192.168.201.202	ET SCAN NMAP OS Detection Probe	11:04 PM
1	Snort	192.168.201.202	192.168.201.145	GPL SHELLCODE x86 inc ebx NOOP	11:04 PM
2	Snort	192.168.201.145	192.168.201.202	ET SCAN Potential SSH Scan OUTBOUND	11:04 PM
2	Snort	192.168.201.145	192.168.201.202	ET SCAN Potential SSH Scan	11:04 PM
3	Snort	192.168.201.145	192.168.201.202	GPL ICMP PING undefined code	11:04 PM
2	Snort	192.168.201.145	192.168.201.202	GPL SCAN nmap fingerprint attempt	11:04 PM
2	Snort	192.168.201.145	192.168.201.202	GPL SCAN nmap fingerprint attempt	11:04 PM
2	Snort	192.168.201.145	192.168.201.202	GPL SCAN nmap XMAS	11:04 PM
2	Snort	192.168.201.145	192.168.201.202	GPL SCAN nmap fingerprint attempt	11:04 PM
3	Snort	192.168.201.202	192.168.201.145	GPL ICMP_INFO Destination Unreachable Port Unreachable	11:04 PM
2	Snort	192.168.201.145	192.168.201.202	ET SCAN NMAP -sS window 1024	11:04 PM
2	Snort	192.168.201.202	192.168.201.145	ET POLICY Reserved Internal IP Traffic	11:04 PM
2	Snort	192.168.201.145	192.168.201.202	ET POLICY Reserved Internal IP Traffic	11:04 PM
2	Snort	192.168.201.145	192.168.201.202	ET POLICY Suspicious inbound to mySQL port 3306	11:04 PM

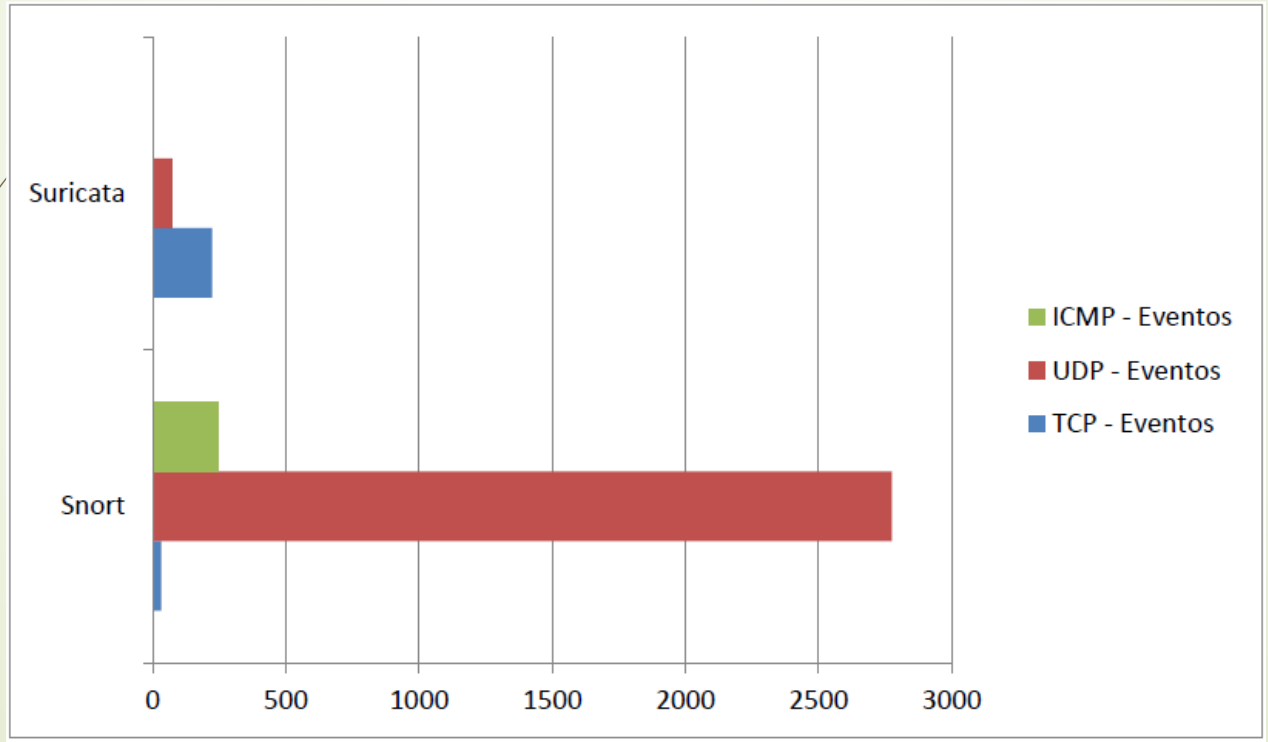
Resultados – Ambiente Virtualizado

Suricata – *Brute Force*

2	Suricata	192.168.201.145	192.168.201.130	ET SCAN Potential SSH Scan OUTBOUND	10:59 PM
2	Suricata	192.168.201.145	192.168.201.130	ET SCAN Potential SSH Scan OUTBOUND	10:59 PM
2	Suricata	192.168.201.145	192.168.201.130	ET SCAN Potential SSH Scan	10:59 PM
1	Suricata	192.168.201.145	192.168.201.130	GPL SHELLCODE x86 inc ebx NOOP	10:59 PM
2	Suricata	192.168.201.145	192.168.201.130	ET SCAN NMAP OS Detection Probe	10:59 PM
1	Suricata	192.168.201.130	192.168.201.145	GPL SHELLCODE x86 inc ebx NOOP	10:59 PM
2	Suricata	192.168.201.145	192.168.201.130	ET SCAN Potential SSH Scan OUTBOUND	10:59 PM
2	Suricata	192.168.201.145	192.168.201.130	ET POLICY Suspicious inbound to mySQL port 3306	10:58 PM

Resultados – Ambiente em produção

Protocolos



Resultados – Ambiente em produção

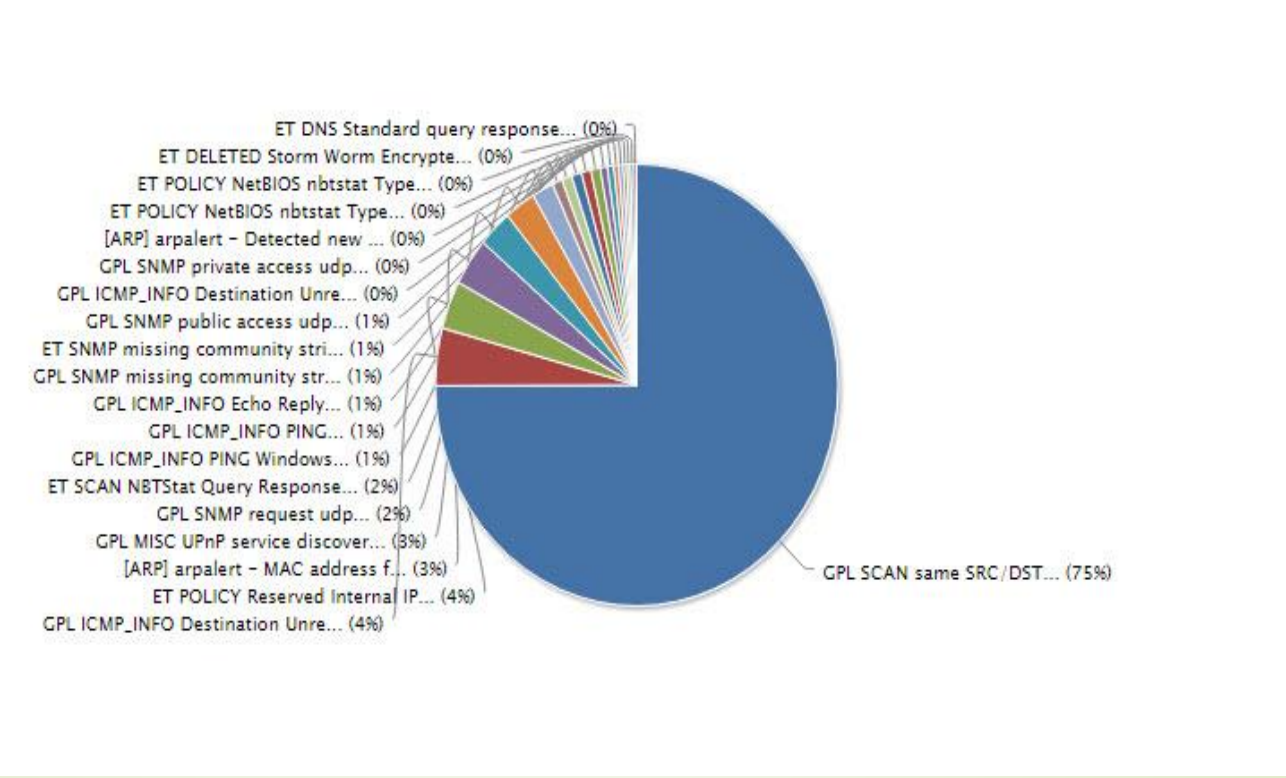
Snort - Pacotes / Categorias de alertas

Resultados – Ambiente em produção

Suricata - Pacotes / Categorias de alertas

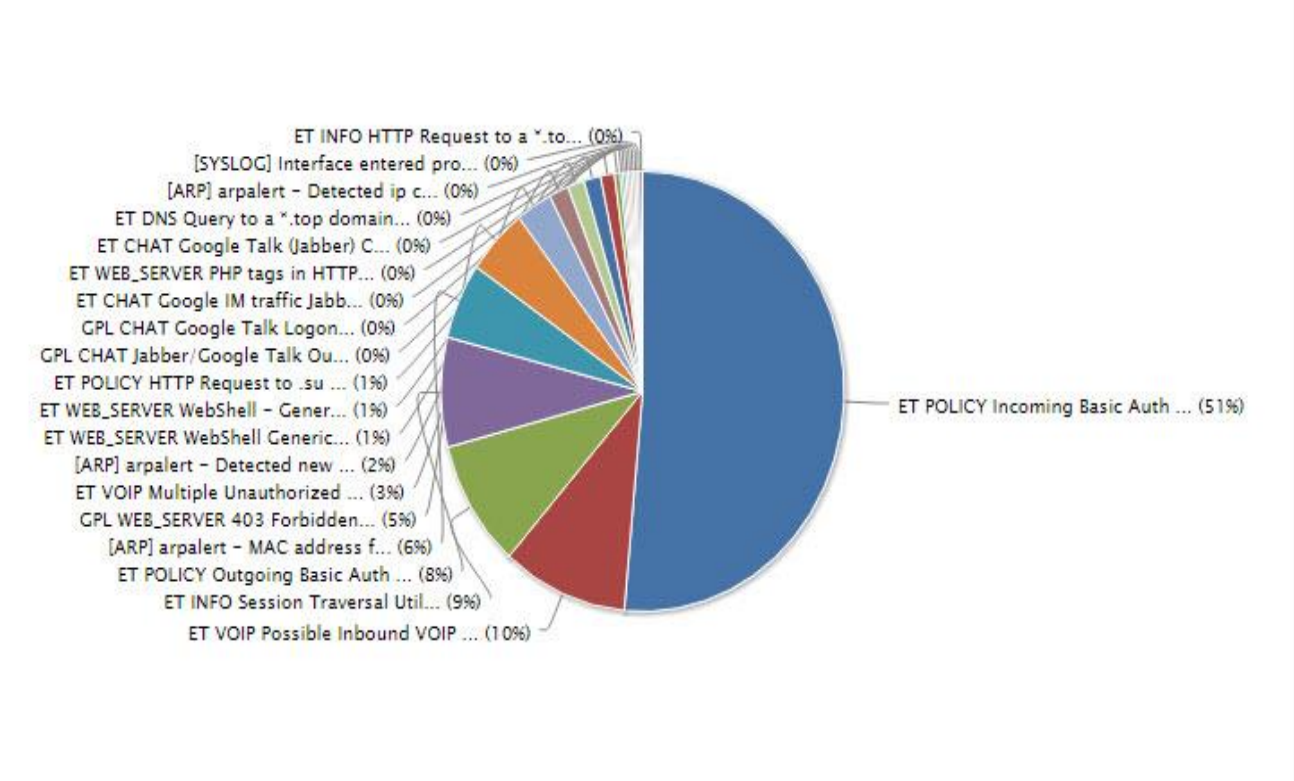
Resultados – Ambiente em produção

Snort – Registros de pacotes



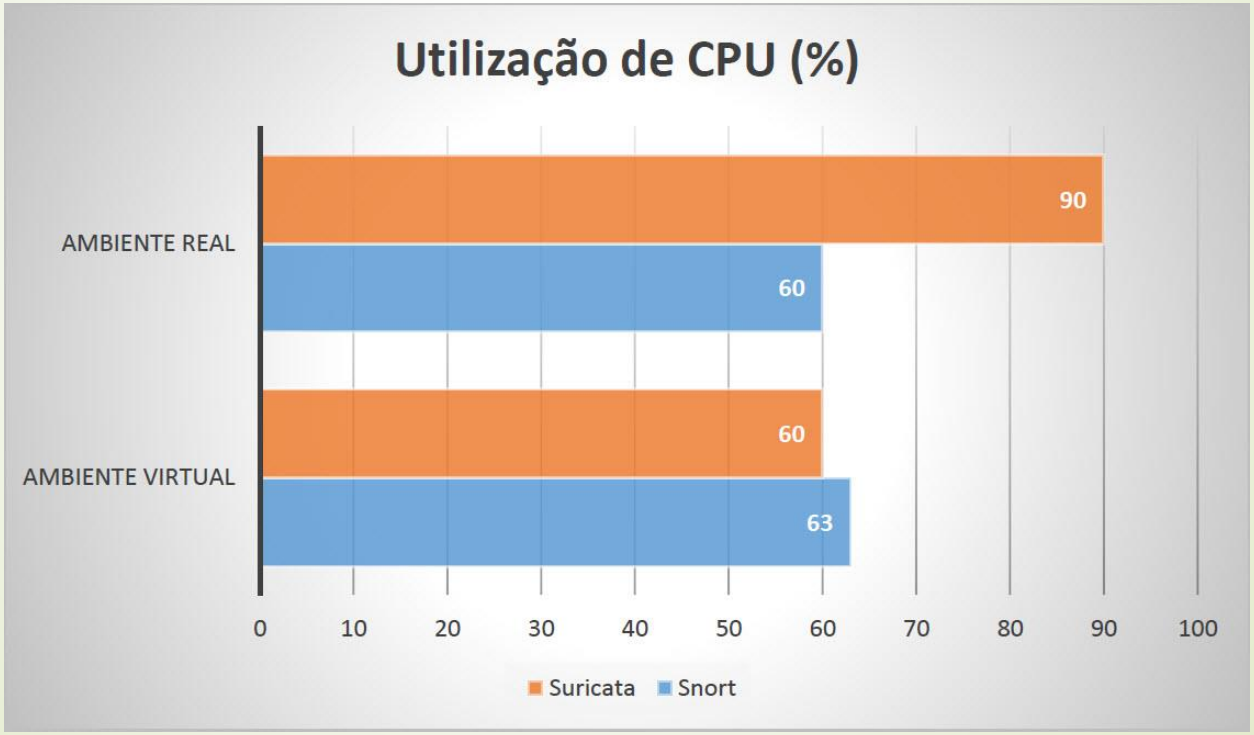
Resultados – Ambiente em produção

Suricata – Registros de pacotes



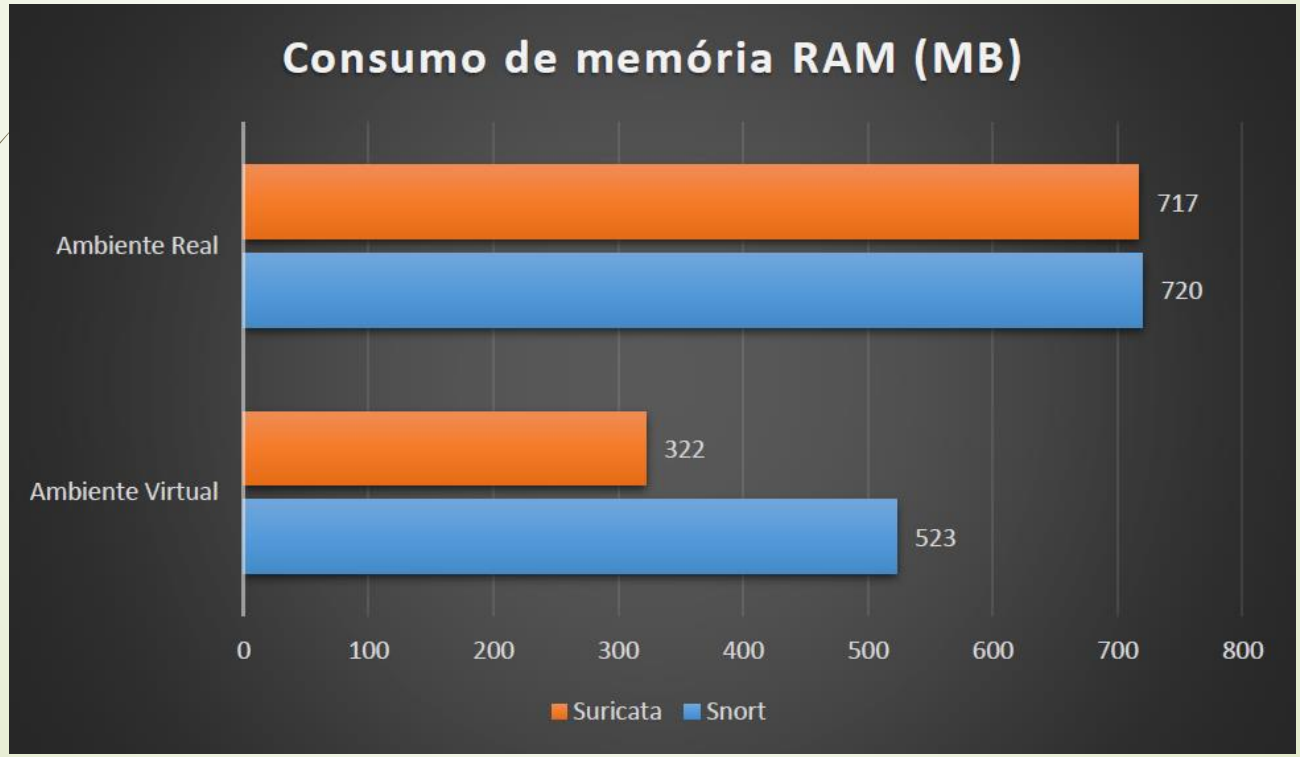
Resultados

Uso de processador (%)



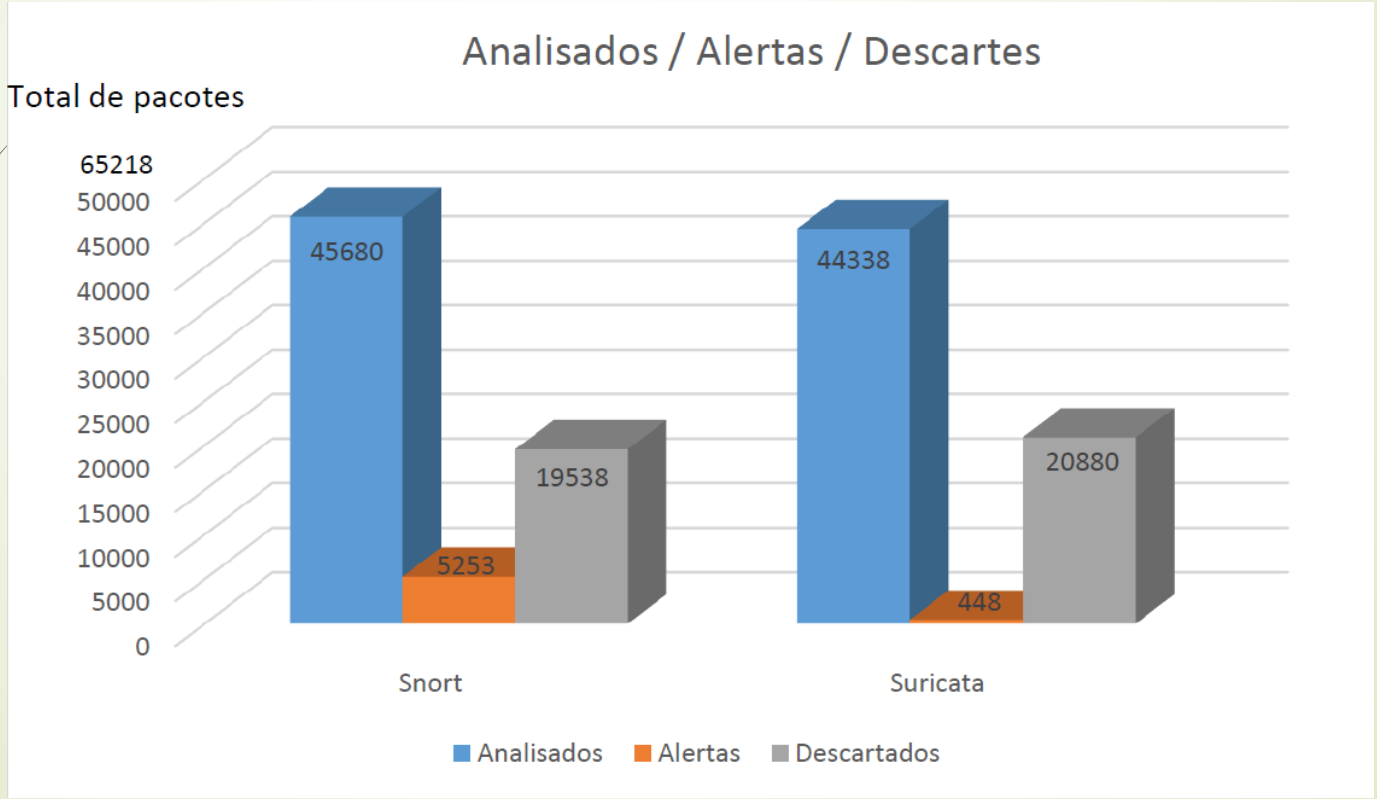
Resultados

Consumo de memória (MB)



Resultados

Volume de pacotes



Conclusões

- O Snort foi mais assertivo, possui mais documentação disponível, tanto no site do mantenedor, quanto de estudos já realizados.
- Quanto ao desempenho, nenhum dos sistemas ficou em destaque.
- Quanto ao volume de pacotes analisados e ao número de alertas gerados, o Snort também foi mais eficiente.

Wiki

- LINK PROPOSTA “EXTERNO”: http://187.7.106.14/wiki2017_1/doku.php?id=projeto08:proposta

- LINK PROPOSTA “INTERNO”: http://192.168.200.3/wiki2017_1/doku.php?id=projeto08:proposta