Suricata & AWS

Pre and Post Session Mirroring
- Overview of Suricata in AWS
- Some lessons learned
- Sharing is caring
- Community feedback
- AWS course
net.ipv4.ip_forward=1
- Hard to size correctly
- Multi-AZ Deployment (still, single point of failure)
- Cost (instance type & multiple instances)
- Limited visibility (no lateral)
## Flow Log Contents

<table>
<thead>
<tr>
<th>Version</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account ID</td>
<td>379063898357</td>
</tr>
<tr>
<td>Interface ID</td>
<td>eni-04b10a1942977452f</td>
</tr>
<tr>
<td>Source Address</td>
<td>172.16.254.34</td>
</tr>
<tr>
<td>Destination Address</td>
<td>32.68.32.56</td>
</tr>
<tr>
<td>Source Port</td>
<td>36490</td>
</tr>
<tr>
<td>Destination Port</td>
<td>443</td>
</tr>
<tr>
<td>Protocol</td>
<td>6</td>
</tr>
<tr>
<td>Packets</td>
<td>77</td>
</tr>
<tr>
<td>Bytes</td>
<td>5040</td>
</tr>
<tr>
<td>Start</td>
<td>1560385064</td>
</tr>
<tr>
<td>End</td>
<td>1560385070</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Log Status</td>
<td>OK</td>
</tr>
</tbody>
</table>

- **VPC Flow Logs version**
- **AWS account ID for the flow log**
- **Source and Destination IPv4/IPv6 Address**
- **IANA protocol number of the traffic**
- **Time, in Unix seconds, of the start/end of the capture window**
- **Status of the log: OK, NODATA, or SKIPDATA**

**Source:** AWS re:Inforce 2019: SEP209 (Youtube)
- Used as a building block
- Excellent tool for troubleshooting
- Security Groups & Network ACL’s
- Agents
- Traffic duplication at OS level
- Next-gen `<buzzword>` mirroring tech
- COST!
“Our number one tenet is to not cause harm or an availability impact; none of the cloud visibility solutions previously available allowed us to be non intrusive...until now.”

Dave Burke, Principal Security Engineer, Amazon.com
$ cat nsm-aws-mirror.txt | more
- No longer inline
- No more traffic duplication at OS
- No agents/maintenance
- Capture at the Elastic Network Interface level
- LATERAL MOVEMENT!
- Cost
- Visibility into often missed log-centric tools
- _insert_reason_why_we_love_NSM
TARGET
FILTER
SESSIONS

Icons from ultimatearm & Nikita Golubev @ flaticon.com
- Elastic Network Interface
- Not everything with an ENI, though
- EC2 and Network Load Balancer
- No 1:1; Target can be used by several Sessions
- UDP 4789 (VXLAN) in SG
- Inbound or Outbound
- Protocol-based (TCP/UDP) filtering
- Source & Destination
- CIDRs supported
- Port (for both SRC and DEST)
- Up to 3 sessions per source (*ENI*)
- Lower session has priority (packets are mirrored only once)
  - #1 - HTTP -> Sensor01
  - #2 - HTTPS -> Sensor02
  - #3 - ALL -> Sensor03
- Launch your instance

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>vCPUs</th>
<th>Memory (GiB)</th>
<th>Storage</th>
<th>EBS Only</th>
<th>Root Access</th>
<th>Network Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>c5n.large</td>
<td>2</td>
<td>5.25</td>
<td>EBS only</td>
<td>Yes</td>
<td></td>
<td>Up to 25 Gigabit</td>
</tr>
<tr>
<td>c5n.xlarge</td>
<td>4</td>
<td>10.5</td>
<td>EBS only</td>
<td>Yes</td>
<td></td>
<td>Up to 25 Gigabit</td>
</tr>
<tr>
<td>c5n.2xlarge</td>
<td>8</td>
<td>21</td>
<td>EBS only</td>
<td>Yes</td>
<td></td>
<td>Up to 25 Gigabit</td>
</tr>
<tr>
<td>c5n.4xlarge</td>
<td>16</td>
<td>42</td>
<td>EBS only</td>
<td>Yes</td>
<td></td>
<td>Up to 25 Gigabit</td>
</tr>
<tr>
<td>c5n.9xlarge</td>
<td>36</td>
<td>96</td>
<td>EBS only</td>
<td>Yes</td>
<td></td>
<td>50 Gigabit</td>
</tr>
<tr>
<td>c5n.18xlarge</td>
<td>72</td>
<td>192</td>
<td>EBS only</td>
<td>Yes</td>
<td></td>
<td>100 Gigabit</td>
</tr>
</tbody>
</table>
- Launch your instance
- Name your interfaces
- Launch your instance
- Name your interfaces
- Create your target
- Launch your instance
- Name your interfaces
- Create your target
- Create your filters
- Launch your instance
- Name your interfaces
- Create your target
- Create your filters
- Create your session
Can we make it easier?
Mirror Toolkit

A set of tools to ease the creation of traffic mirror sessions, increase automation and facilitate maintenance.
AutoMirror

- Fully automate session creation
- Automate time consuming tasks (double-check identifiers)
- Allow configuration via standard AWS methods (Tags)
- Set and forget
AutoMirror DEMO

Plan B
Video of a similar demo

https://youtu.be/lZn4KDexC-4
NSM Compliance

- Custom rule for AWS Config
- Automate technical state compliance
- Good fit for AutoMirror
- Can be used separately
AWS Mirror Toolkit

github.com/3CORESec/AWS-Mirror-Toolkit
Traffic counts towards mirror source capacity.

Production traffic > Mirrored Traffic

4GB of traffic for source
2GB of traffic for destination
- Enhanced Networking on Linux
- Powered by Single Root I/O Virtualization (SR-IOV) for lower CPU utilization
- Higher bandwidth, PPS performance and lower inter-instance latency
- Available on Elastic Network Adapters (up to 100 Gbps)
- Example: EC2 C5n - Network Optimized
- Make use of Placement Groups: Cluster

- **Traffic destination:** Network Load Balancer
- **Flow hashing applied to traffic mirror**
  - Protocol (UDP); Source IP; Source Port; Destination IP; Destination Port
- **Behind NLB:** EC2 C5n instances on ASG
- **ASG launches instances with custom AMI**
- **Health check done to TCP port**
- Hub and spoke model
- Replacement of VPC Peering
- Centrally managed routing/policies
- 50 Gbps
Is there a place for NSM in cloud environments?
AWS GuardDuty is a managed service that continuously monitors malicious and unauthorized behaviour to protect AWS accounts, relying on CloudTrail, VPC Flow Logs and DNS logs.
“Threat intelligence coupled with machine learning and behavior models help you detect activity such as crypto-currency mining, credential compromise behavior, communication with known command-and-control servers, or API calls from known malicious IPs.”

Source: https://aws.amazon.com/guardduty/
Example: AutoMirror in IR
$ cat automirror-ir.txt

AutoMirrorIR=True

Instances under investigation

Coming to the toolkit ... Soon!

Ephemeral Suricata

Evidence & Long term storage (PCAP & EVE)
In an environment with properly configured IAM policies and groups, tampering with traffic collection is not possible, making it resilient against manipulation and tampering.
- New way of looking at cloud-based NSM
- Interesting challenges and opportunities
- Serverless visibility?
- HPC NSM (Suricon 2020?)
- New security & networking challenges
Questions?

@0xTF