Ntopng: lighthouse to find the right way to escape from the network fog

FOSDEM2021
Agenda

• Introduction and Motivation
• Use Cases
• Future
• Conclusions
Introduction

- Active on Security Filed since 2001
- Passionate about IT Technology
- Very long field experience

LinkedIn: https://www.linkedin.com/in/giordano-zambelli-a46b673/
Email: Giordano.Zambelli@verxo.it

"Everything I will say is under my direct responsibility"
Introduction

• Networks are growing at very fast rate.
• Network are expanding.
• Smart Working growth.
• Every day more and more new services are implemented using networks.
• Needs of Traffic assurance
• Cyber Security approach needs more insight
• New Cyber Security paradigm to approach
Introduction

Tipical «customer-supplier» conversation.

◦ Customer: «Hey Guys, it seems that there are something wrong on the network!»

◦ ..... 

◦ Tech: «Have you some metrics out of range?»

◦ ..... 

◦ Customer: «No, but in my opinion, something is not working as expected!»

◦ Tech: «Wait, please. I need to check ntopng»
Case 1

Customer Problem: Download fails

1. Packet Evidence:

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Destination Address</th>
<th>Protocol</th>
<th>Port</th>
<th>SID</th>
<th>Packet Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>bouncer-bouncer</td>
<td>10.41.0.128</td>
<td>TCP</td>
<td>443</td>
<td>49572</td>
<td>55 [TCP Keep-Alive] 443 + 49572 [ACK] Seq=4408 Ack=1476 Win=29696 Len=0</td>
</tr>
<tr>
<td>cdn-proxy-prod</td>
<td>10.41.0.128</td>
<td>TCP</td>
<td>443</td>
<td>49574</td>
<td>55 [TCP Keep-Alive] 49545 + 443 [ACK] Seq=2541 Ack=1765 Win=258 Len=1</td>
</tr>
<tr>
<td>skypedataprdcol</td>
<td>10.41.0.128</td>
<td>TCP</td>
<td>443</td>
<td>49574</td>
<td>60 [TCP Keep-Alive] 443 + 49545 [ACK] Seq=1765 Ack=2542 Win=234 Len=0</td>
</tr>
</tbody>
</table>

2. Security Services on the Middle operated by Perimeter Firewall (AV Module fails)

Result: ntopng alert: Low Goodput
Case 2

Customer Needs: Verify Security Effectiveness

Be sure GeoIP Filtering is working on the perimeter. Internal Client to External Blacklisted Country Server

1. Alarm Evidence: Flow alert: Internal IP is calling

![Image of flow alert]

2. GeoIP Filtering not working. Ntopng alert: BlackListing Country (Custom Country list)
Case 3


Requirements

1. ntopng engines (Mirror plus nprobe)
2. MS Azure Sentinel Subscription

GOALS: Internal traffic alerts shared with Sentinel Correlation Engine (Lateral movements, VPN, etc).
Case 3

Sentinel Log:

{"alert_tstamp":1606985707,"alert_entity_val":"1X.1xx.2xx.1xx@0","ifid":6,"alert_granularity":60,"action":"release","alert_entity":1,"alert_subtype":"flow_flood_victim","pool_id":1,"alert_type":11,"alert_tstamp_end":1606985766,"message":"[03/12/2020 09:56:06] [ens3f0] [Flows Flood] [Released] Host 1x.1xx.2x.1xx [BLABLA04] Local is under flow flood attack [10000 > 5000 flows received]","alert_json":"{"alert_generation":{"confset_id":0,"host_info":{"systemhost":false,"is_blacklisted":false,"host_services_bitmap":14,"localhost":true},"script_key":"flow_flood_victim","subdir":null,"host":null,"operator":"gt","threshold":100,"metric":"flow_flood_victim","value":101},"alert_severity":5}
Case 4

Customer Scenario: Wireless ISP

Customer Problem: user complains about slow bandwidth

Enduser CPE Monitoring

Ntopng view: Customer compromised?
Case 5

Customer Scenario: Enterprise
Customer Problem: user complains about service unavailability

Wrong DNS settings on DHCP??
FUTURE

Customer Scenario: Zero trust paradigm

Customer Problem: Monitoring Zero trust architecture

Zero trust

[Diagram comparing Traditional TCP/IP and Software-Defined Perimeter]
Conclusion

an IT Swiss Knife!!