VERXO

Verso una sicurezza totale

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

FOSDEM2021

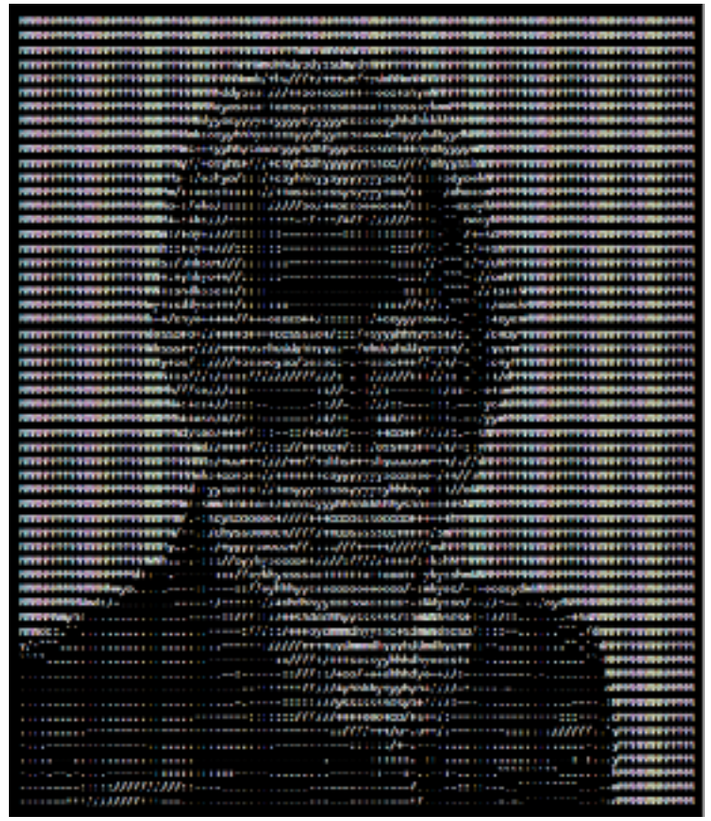
ntop

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:

113…	07:30:31,760619	bouncer-bouncer…	443	10.41.0.128	TCP	49572	60 [TCP Keep-Alive ACK] 443 → 49572 [ACK] Seq=4408 Ack=1476 Win=29696 Len=0
113…	07:30:32,042976	10.41.0.128	49557	srv.14.northeuro…	TCP	443	55 [TCP Keep-Alive] 49557 → 443 [ACK] Seq=3467 Ack=4884 Win=66048 Len=1
113…	07:30:32,044682	srv.14.northeur…	443	10.41.0.128	TCP	49557	60 [TCP Keep-Alive ACK] 443 → 49557 [ACK] Seq=4884 Ack=3468 Win=61952 Len=0
113…	07:30:32,058541	10.41.0.128	49545	srv.14.northeuro…	TCP	443	55 [TCP Keep-Alive] 49545 → 443 [ACK] Seq=2541 Ack=1765 Win=258 Len=1
113…	07:30:32,060159	srv.14.northeur…	443	10.41.0.128	TCP	49545	60 [TCP Keep-Alive ACK] 443 → 49545 [ACK] Seq=1765 Ack=2542 Win=234 Len=0
113…	07:30:32,214549	10.41.0.128	49574	cdn-proxy-prod.s…	TCP	443	55 [TCP Keep-Alive] 49574 → 443 [ACK] Seq=1218 Ack=2740267 Win=169728 Len=1
113…	07:30:32,216370	cdn-proxy-prod.…	443	10.41.0.128	TCP	49574	60 [TCP Keep-Alive ACK] 443 → 49574 [ACK] Seq=2883604 Ack=1219 Win=59392 Len=0
113…	07:30:32,791785	10.41.0.128	49556	skypedataprdcolc…	TCP	443	55 [TCP Keep-Alive] 49556 → 443 [ACK] Seq=49676 Ack=10096 Win=65792 Len=1

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

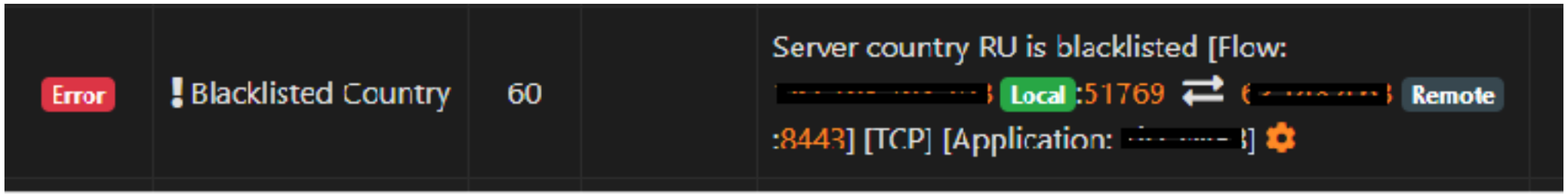
Result: ntopng alert: Low Goodput

Case 2

Customer Needs: Verify Security Effectivness

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

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



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

Case 3

Customer Scenario: about 65 Branches. Microsoft Azure Sentinel like SIEM with ntopng as network sensor.

Requirements

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

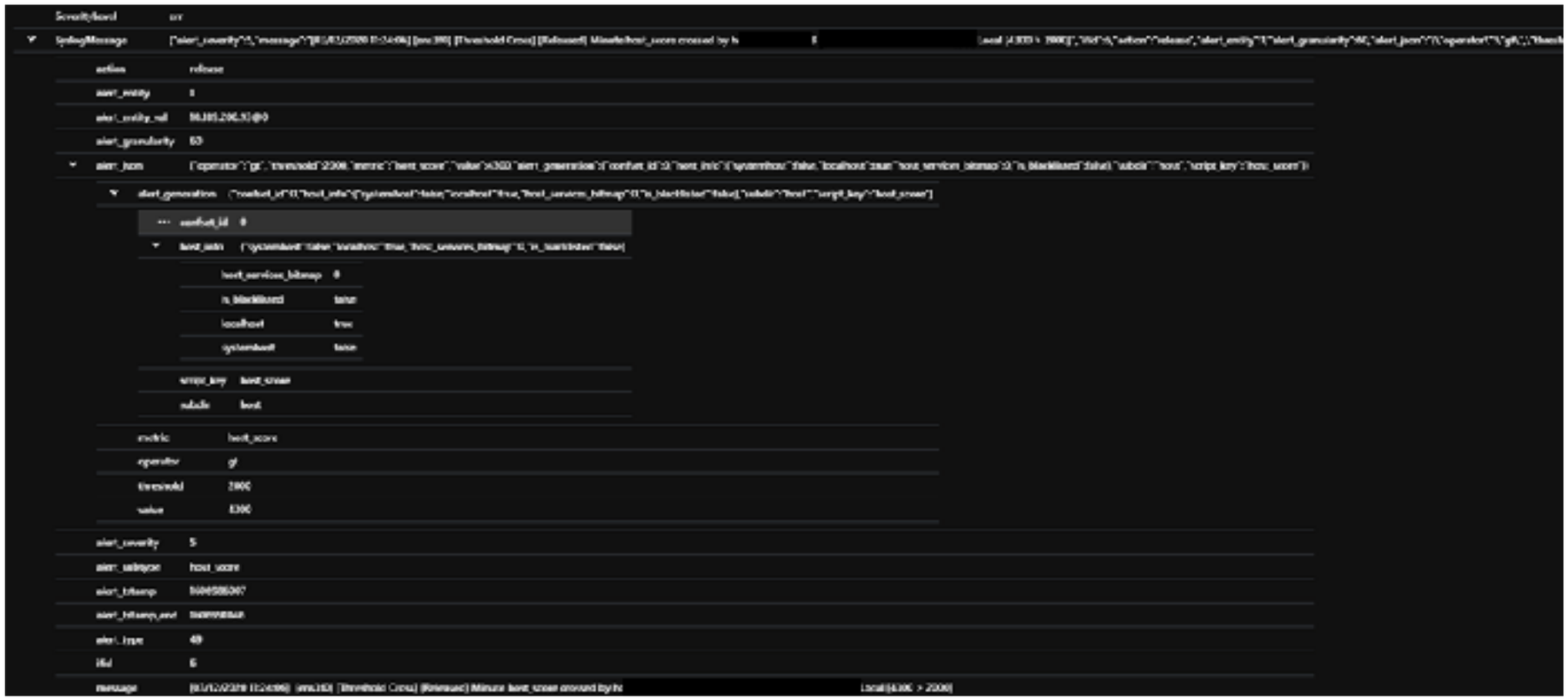
GOALS: Internal traffic alerts shared with Sentinel Correlation Engine (Lateral movements, VPN, etc).

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\":

\"host\"},\"operator\":\"gt\",\"threshold\":100,\"metric\":\"flow_flood_victim\",\"value\":101}","alert_severity":5}

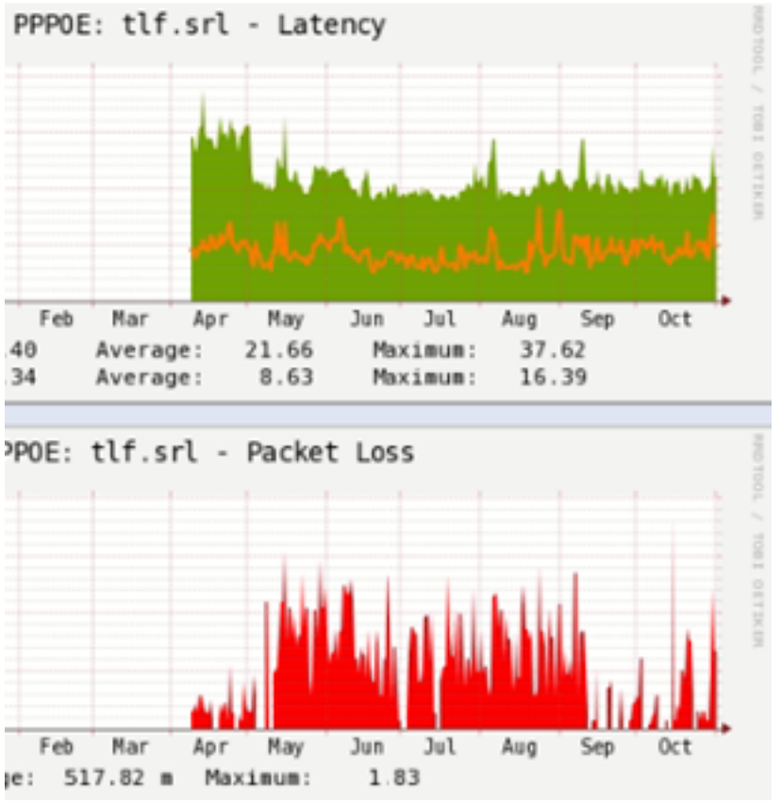


Case 4

Customer Scenario: Wireless ISP

Customer Problem: user complains about slow bandwidth

Enduser CPE Monitoring



Ntopng view: Customer compromised?

Application	Protocol	VLAN	Client	Server	Duration
Unknown	TCP	243	[redacted]:45946	45.129.33.125:56388	< 1 sec
Unknown	TCP	243	[redacted]:40803	45.129.33.127:56328	< 1 sec
Unknown	TCP	243	[redacted]:47104	45.129.33.124:56416	< 1 sec
Unknown	TCP	243	[redacted]:2020	103.125.191.54:59865	< 1 sec
Unknown	TCP	243	[redacted]:430	45.146.165.160:43891	< 1 sec
Unknown	TCP	243	[redacted]:842	45.146.165.160:43891	< 1 sec
Telnet	TCP	243	[redacted]:telnet	localhost:58498	< 1 sec
Unknown	TCP	243	[redacted]:44731	45.129.33.125:56388	< 1 sec
Unknown	TCP	243	[redacted]:40803	45.129.33.127:56328	< 1 sec
Unknown	TCP	243	[redacted]:40031	45.129.33.127:56328	< 1 sec
Unknown	TCP	243	[redacted]:47104	45.129.33.124:56416	< 1 sec

Case 5

Customer Scenario: Enterprise

Customer Problem: user complains about service unavailability

Wrong DNS settings on DHCP??

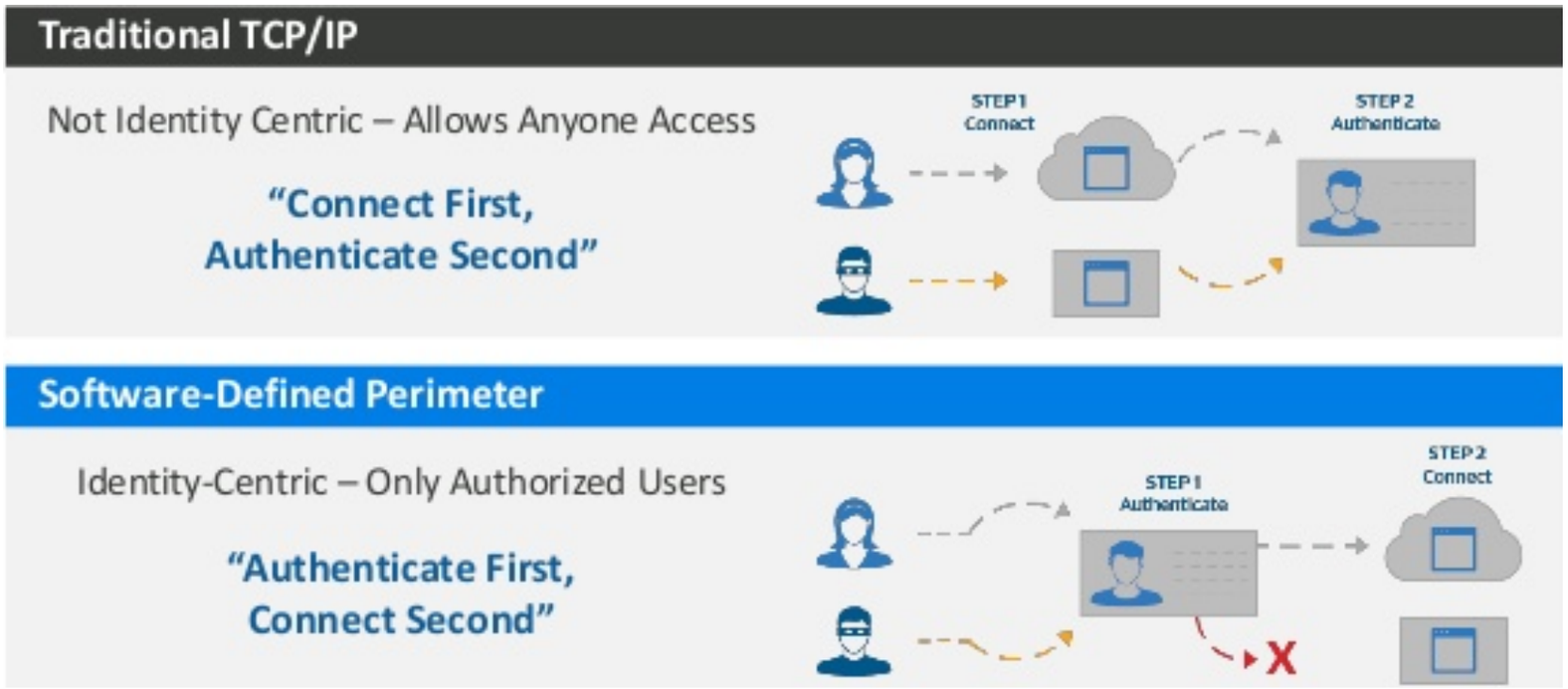
! Unexpected DNS found	100		Unexpected DNS server found: [redacted] [Flow: [redacted] Local :53 ⇄ [redacted] Local :58030] [UDP] [Application: DNS]
! Unexpected DNS found	100		Unexpected DNS server found: 192.168.168.101 [Flow: [redacted] Local :53 ⇄ [redacted] Local :53732] [UDP] [Application: DNS]
! Unexpected DNS found	100		Unexpected DNS server found: 192.168.168.101 [Flow: 8.8.8.8 Remote :53 ⇄ [redacted] Local :53732] [UDP] [Application: DNS.Google]
! Unexpected DNS found	100		Unexpected DNS server found: 192.168.168.102 [Flow: [redacted] Local :53 ⇄ [redacted] Local :52330] [UDP] [Application: DNS]

FUTURE

Customer Scenario: Zero trust paradigm

Customer Problem: Monitoring Zero trust architecture

Zerotrust



Conclusion

an IT Swiss Knife!!