ntopng: Traffic Analysis and Flow Collection

News and Updates

Matteo Biscosi
Veronika Anistratova
Agenda

• ntopng: What's changed
  • Anomalies & Behavior Analysis
  • Score indicator
  • Alerts Development, Find the problem
  • Checks Extended, Road to Cybersecurity
  • Endpoints
  • ...

• ntopng: Towards Dynamic UX
Anomalies & Behavior Analysis
Anomalies & Behavior Analysis [1/6]

- Analyze the current behavior of Hosts and try to find anomalies in its future behavior -> Prevention

- Analyze the current behavior of Hosts and understand if unwanted (malicious) traffic is seen on an interface
Anomalies & Behavior Analysis [2/6]

**Anomaly!**

**Unexpected Behavior!**
Anomalies & Behavior Analysis [3/6]

- Two new ways to analyze unwanted traffic:
  - Service Map: analyze local traffic to find unwanted local services (Lateral Movements)
  - Periodicity Map: analyze traffic to find unwanted periodic flows (e.g. BotNet)
Anomalies & Behavior Analysis - Service Map [4/6]

- Learning Period in order to decide which local services are right and which not

- Trigger an alert if non-right services are seen from ntopng

Unwanted Traffic!
Anomalies & Behavior Analysis - Service Map [5/6]

- Analyze the Degree - number of connections it has to other node: is it alright to have that number of Edges? Why is this Host in the local services?
Anomalies & Behavior Analysis - Periodicity Map [6/6]

- Analyze periodic flows:
  - "Is it normal to have the same flow every 20 seconds?"
  - "Is it normal to have seen the same flow for over 500 times?"
Score Indicator
Score [1/2]

• The score is a numerical indicator that when non-0 it indicates that some kind of issue is present: the higher is the score the worst is the problem:

• The **flow score** that indicates how bad is this flow

• The **host score** is computed as the sum of all active flow scores (either as client or server) plus additional scores eventually found on the host
Score [2/2]

Probably Attacked/er!
Alerts Development, Find the problem
Alerts Development, Find the problem [1/3]

• Analyze the traffic to find problems in a few click!

• Analyze live flows and other to trigger alerts based on different anomalous metrics and classify them based on the severity of the problem
Alerts Development, Find the problem

[2/3]

System

Host

Flows
Alerts Development, Find the problem [3/3]

- Find the problems you are interested in, by filtering the records

- Remove the "False positive" from your system
Checks Extended, Road to Cybersecurity
Checks Extended, Road to Cybersecurity [1/4]

• What is a Check? A check is a part of a verification process integrated in Ntopng that is able to detect a certain condition, like an host/network anomaly or device malfunctioning. Once seen the deviation, the references are passed in order to create an alert.

• But how an alert is created?
  
  • When a threshold is crossed (More traffic then expected, Score higher then expected, ...)
  
  • When an anomalous situation is detected on the packets (Malformed packets, Suspicious contents, ...)
  
  • When a scan is detected (ICMP, SYN, ...)
  
  • When unwanted traffic is detected (Bot, Binary Transfers, ...)
  
  • When unexpected Hosts are detected in a network (DNS Servers, NTP Servers, ...)

Checks Extended, Road to Cybersecurity [2/4]

• Alerts are divided by families; there are different alert families in ntopng, each one detecting a different type of alert:

  • Host (IPv4 or IPv6 address)

  • Interface (hardware attached to devices to allow them to communicate over a network)

  • Local Network

  • SNMP Device (Enterprise License)

  • Flow

  • System (The system on top of which ntopng is running; e.g., disk space and load)

  • Syslog (They are not real checks but rather are triggered whenever a syslog entry is received from another device, e.g., firewall logs)
Checks Extended, Road to Cybersecurity [3/4]

- Other then families we have categories. An alert could be an alert related to a Local Network but it could be even a Cybersecurity alert!

- An alert has two classification: an Alert Family and a Category

- Categories:
  - Active Monitoring
  - Intrusion Prevention and Detection
  - Internals
  - Network
  - Cybersecurity
  - SNMP
  - System
Checks Extended, Road to Cybersecurity [4/4]

- More then 100 available checks!

- Check the documentation for more info: https://www.ntop.org/guides/ntopng/alerts/host_checks.html
Endpoints: Integration with External Tools
Endpoints

- Extended the possibility to export Alerts to external tools:
  - Discord
  - ElasticSearch (Pro License)
  - E-Mail
  - Fail2Ban (Pro License)
  - Shell Script
  - Slack
  - Syslog
  - MS Teams (Pro License)
  - Telegram
  - Webhook
ClickHouse
ClickHouse [1/3]

- New Support to a DB: ClickHouse (Enterprise License)
- High Speed Relational Database
- Used to store both Alerts and Flows
  - Historical Flow page -> Ability to navigate the records and find various data:
    - Top Talkers
    - Top Clients
    - Top Applications
    - ...

June, 23-24 · Milan
ClickHouse [2/3]

- Navigate the Historical Flows, find the problems and strange traffic, by filtering them and using the aggregated data we provide (Enterprise License)
ClickHouse [3/3]

- Find the problems by starting from less granular data then tables!
Find the problem
From the great to the small
Find the problem [1/2]

Alerts
Analyze problems starting from the alerts:
Why is there this alert?

↓

Historical Flows
Find the problematic flow:
Who caused the problem?
Is there someone else creating the same problem?
Which type of traffic is this Host doing?

↓

Granular analysis
Find the problem [2/2]

- Analyze the Flow in details and find the problem!
Active Monitoring
Active Monitoring [1/2]

• ntopng is not just a passive monitoring tool!

• Various types of active monitoring:
  • ICMP
  • Continuous ICMP
  • HTTP
  • HTTPS
  • Throughput
  • Speedtest
  • SNMP
Active Monitoring [2/2]
ntopng: SNMP
SNMP: Analysis

• Neighbouring information allows to discover adjacencies and this the topology (Enterprise License).

• This information is present in the data link layer (layer 2).

• Vendors have their own protocols (e.g. Cisco has CDP Cisco Discovery Protocol) but the standard is LLDP Link Layer Discovery Protocol (RFC 2922)
  
  • LLDP periodically send LLDP packets with multicast. Information on neighbour devices can be read using SNMP (LLDP-MIB).
SNMP: Bridge MIB

- Useful for controlling the status of L2/L3 switches. Do not make the common mistake to believe that it is used only on bridges.

- It somehow complementary to the MIB II as it provides information the hosts connected to the switch ports.

- Common uses of the bridge MIB:
  - To know the MAC address of a host connected to the port X/unit Y of the switch.
  - The MAC/port association is the base for detecting the physical location of a host (good method for know who’s where!)
  - It keeps track of the “previous” MAC address (and the time) connected to a port so it is possible to track users as they move from a room to another
  - It can be used for detecting ports with associated multiple MAC addresses (trunk) hence to detect users with multiple MACs (e.g. VM and PC infected by a virus/worm)
SNMP: Map

- With all this information we can create Maps:
  - Who's talking with who?
  - Where are they located?
ntopng and nProbe
ntopng and nProbe: IPS Mode

- ntopng can be used to enforce traffic policies and report them, when ntopng is used in combination with nProbe in IPS mode.

- Traffic policies are automatically exported to nProbe after a change to the policies configuration. Rules that can be used to configure exceptions are:
  
  - L7 Application Protocol Rules
  - L7 Category Rules
  - Host Rules to configure hostnames used in TLS and DNS protocols for instance
  - Country Rules
  - Continent Rules
  - Risk Rules to apply policies based on the Flow Risk computed by nDPI
ntopng and nProbe: Processes

- ntopng can be used in combination with nProbe in Agent Mode to understand which processes the nProbe host machine is running.
- Find the compromised machine and who's the culprit!
ntopng Edge

Protects all of your digital assets and online activities
ntopng nEdge

• Support for latest Ubuntu Server 22 LTS

• Improvements for multi-WAN environments for gateway selection (e.g. connectivity provider with 3G, WiFi, SAT)
ntopng: Towards Dynamic UX
ntopng GUI

• We have news even from the Web Interface!

• We are renewing the front-end by moving to a dynamic GUI:
  • Better Performances even from the Web Interface
  • Possibility to export our components into external tools
ntopng: Dynamic UI

• With the help of Vue.js we are trying to:
  
  • Have lesser loading, by loading only the needed components (from static to dynamic UI) -> better performances and user experience
  
  • Create bundles that other tools could import and use our components into their own page -> Create your custom dashboard!
thank you

https://github.com/ntop/ntopng

ntopConf’22