ntopng

Einführung in ntopng und Anwendungsfälle

Tobias Goller

Würth Phoenix Solution Architect

Agenda

- Was ist ntopng
- Netzwerkanalyse und Architektur einer ntopng Umgebung
- Anwendungsfälle von ntopng
- Woher erhalte ich ntopng
- Live demo

Was isT ntopng

ntopng ist eine webbasierte Hochgeschwindigkeits-Verkehrsanalyse und Datenflusserfassung.

ntopng wird von einer Softwarefirma aus Pisa, Italien unter der Leitung con Luca Deri entwickelt.

Einige Hauptfunktionen

- Sammeln von Netzwerkverkehr (SPAN Port, NetFlow, sFlow oder IPFIX)

- Web GUI

- Anzeige des Netzwerkverkehrs in Echtzeit mit den aktiven Hosts

- Sortierung des Netzwerkverkehrs nach vielen Kriterien, einschließlich IP-Adresse, Port, Layer-7 (L7), Anwendungsprotokollen, Durchsatz, autonomen Systemen (ASs).

- Erstellung von Langzeitberichten für verschiedene Netzwerkmetriken, einschließlich Durchsatz und L7-Anwendungsprotokolle

- Top-Talker (Sender/Empfänger), Top-ASs, Top-L7-Anwendungsprotokolle

- Hosts geolokalisieren und in einer geografischen Karte überlagern

- Flexible Handhabung von Warnungen durch ein Alarmierungssystem mit externen Endpunkten (Slack, Email, Webhook, …)

- Layer-7-Anwendungsprotokolle entdecken (Facebook, YouTube, BitTorrent usw.)

- Deep Packet inspection mittels nDPI

- Fokussiert auf Verkehrstransparenz, Cybersicherheit und Malware detection

- Network Device Discovery

Einige Hauptfunktionen

Durch den Einsatz von ntopng können folgende und weitere Probleme analysiert und erkannt werden.

- Welche Verbindungen habe ich in meinem Netzwerk (wer mit was zu wem, usw).
- Bandbreiten Analyse
- SLA Überwachungen mit Providern
- Internet ist langsam oder ist nicht verfügbar
- Status der Switche und Router
- Ist mein Netzwerk sicher (cybersecurity)
- Welche Geräte sind in meinem Netzwerk

Analyse der Flüsse/Flows

Was ist ein Fluss/Flow:

Ein Fluss ist eine Paketzusammenfassung, die die Kommunikation darstellt.

Ein Fluss/Flow besteht aus allen Paketen, welche eine Verbindung darstellen.

Typischerweise wird ein Fluss/Flow aus folgenden Einheiten identifiziert.

- src und dst IP‘s
- src und dst Ports
- Layer 4 protocol (z.B. TCP, UDP)
- Andere Informationen (z.B. VLAN)
- Metadaten (z.B. Layer 7 Informationen)

Wie kann ich die Pakete aus meinem Netzwerk sammeln?

- **netflows** (ein Gerät, z.B. ein Switch sendet netflows zum ntopng Gerät)

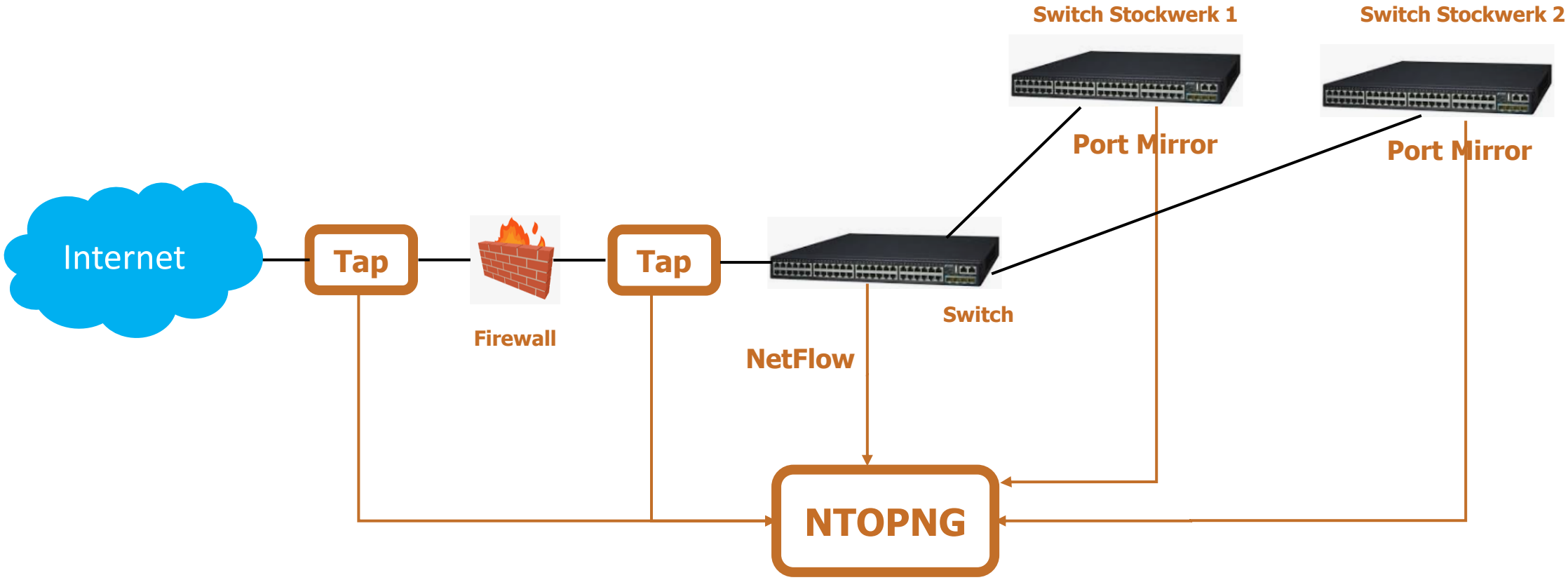
- **Port Mirror/SPAN** auf dem Netzwerkgerät, z.B. Switch, welcher dann mit dem ntopng Gerät verbunden ist

- **Network TAP** (Ein „Terminal Access Point“ ist in der Regel ein dediziertes Hardwaregerät, das den Zugriff auf die über ein Computernetzwerk fließenden Daten ermöglicht.)

Die Herausforderung für eine optimale Nutzung besteht darin, dass wir verstehen müssen, welche Flüsse angezeigt werden sollen. Dies ist notwendig, um die verschiedenen Sniffer, Packet Sammler oder TAP‘s richtig zu positionieren.

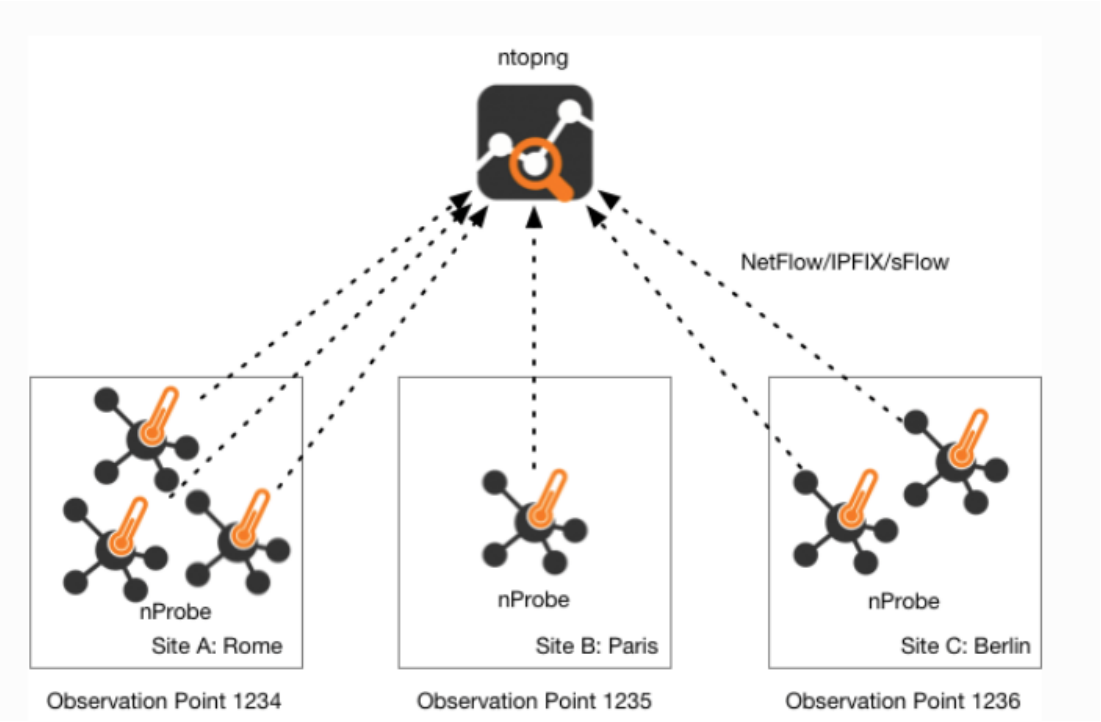
netzwerkanalyse UND Architektur von ntopng

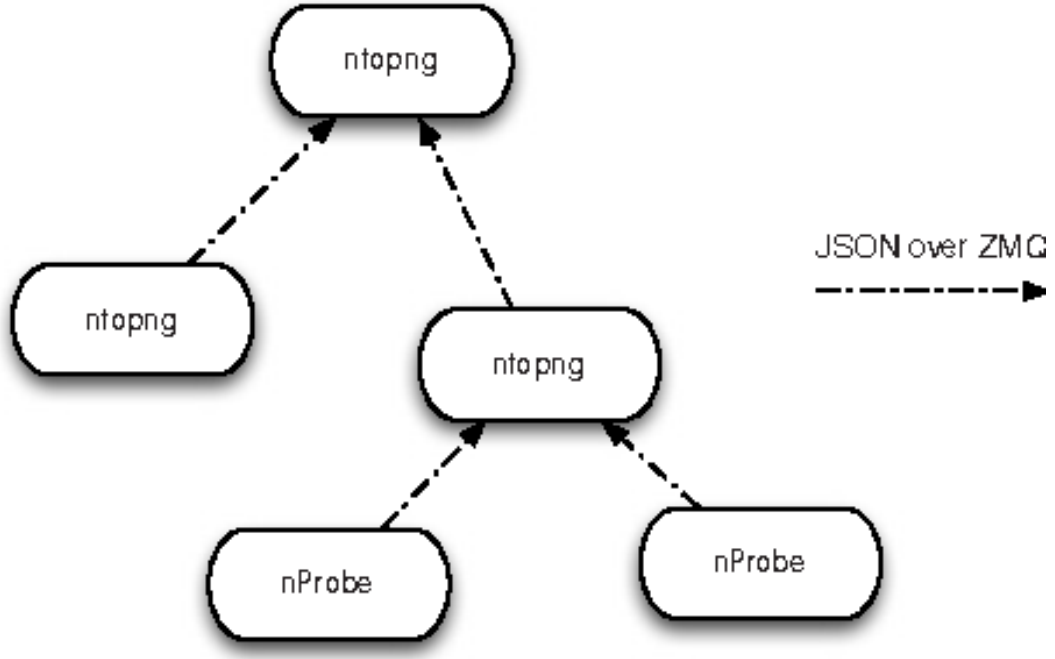
- Grafisches Szenario



netzwerkanalyse UND Architektur ntopng

- Grafische Darstellung einiger möglichen Unternehmensumgebungen mit mehreren nboxen/nprobes und unterschiedlichen eingesetzten Modulen



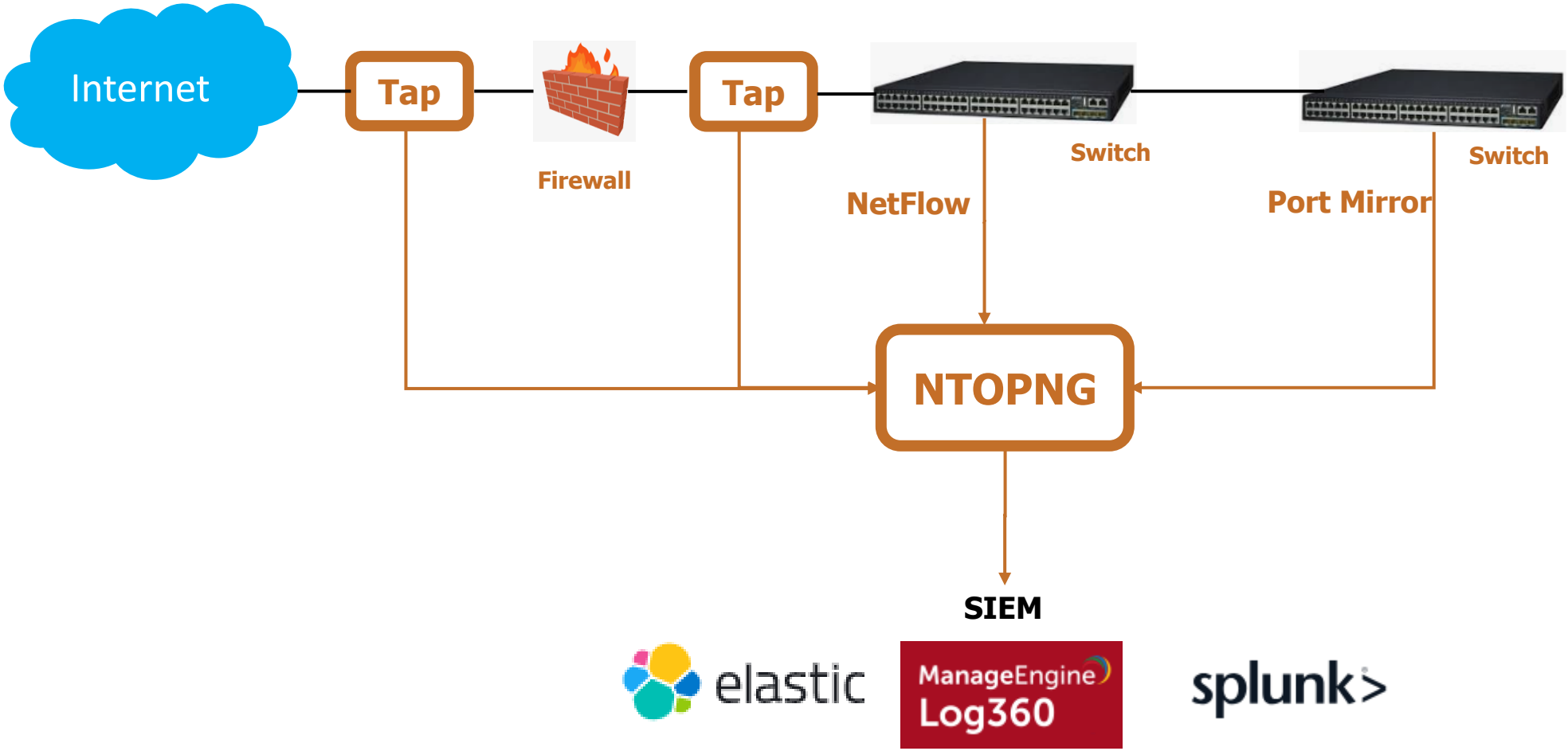


Anwendungsfälle ntopng

- Analyse des Datenverkehrs in Echtzeit mit der Layer-7-Analyse in Ihrem Netzwerk
- Analyse des sortierten IP-Verkehrs nach Quell- und Zieladresse
- Lokalisierung von Hosts auf einer geografischen Karte
- Erstellung von Langzeitberichten für Netzwerkmetriken, einschließlich Durchsatz und L7-Anwendungsprotokolle
- Korrelation des VPN-Benutzerverkehrs
- Integration von Drittanbietern, z.B. influxdb
- PCAP-Dateianalyse
- Verwenden Sie ntopng, um Einbrüche und Netzwerkschwachstellen zu überprüfen
- Verwenden Sie ntopng-Warnungen, um SIEM-Lösungen zu füllen

Anwendungsfälle ntopng

- Mithilfe der ntopng-Alarmierungsregeln können die bereits gefilterten und standardisierten Daten an das SIEM-System gesendet werden. Das bedeutet, dass auf dem SIEM-System keine Rollen oder zusätzliche Filter erforderlich sind.



Woher erhalte ich ntopng

Woher kann ich ntopng erhalten bzw. Wo ist es integriert ?

Module im Neteye

ntopng kann als zusätzliches Modul in eine NetEye-Installation integriert werden.
Mit diesem Modul kann nprobe auch als Datensammler verwendet werden.
(nProbe is a software NetFlow v5/v9/IPFIX probe able to collect, analyze and export network traffic reports using the standard Cisco NetFlow v5/v9/IPFIX format.)

nbox

Mit einer nbox versteht man eine dedizierte Hardware Appliance auf welcher die ntop Software installiert ist. Die Hardware wird dabei genau auf ihre Netzwerkanalyseanforderungen abgestimmt. Dies hat den Vorteil, dass es keine Performance Probleme bei der Analyse und Sammlung von Flüssen gibt.
Weiter können SPAN Ports direkt an diese Appliance angeschlossen und analysiert werden. Auch PCAP Dateien können daraus erstellt werden..

In einer verteilten Umgebung können kleinere nboxen als Sammler verwendet werden und die Daten an eine große nbox gesendet werden, die die Daten korreliert anzeigen kann.

NTOP SOFTWARE

Die ntop Software kann über den ntop Webauftritt oder über Gravitate oder Würth Phoenix gekauft werden.


Fragen ???
live demo