Observability and Large-Network Monitoring Webinar

ntop

Webinar Outline

- ntopng as an Observability Platform
  - From traffic monitoring to real-time observability
  - Fine-grained visibility into micro-bursts and transient anomalies with high-resolution counters
- Large-Network Monitoring
  - Routing & BGP for Large-Scale Networks
  - Monitor routing health, visualize BGP paths, gain actionable insights

Traditional Monitoring Is Not Enough

- Traditional monitoring platforms typically aggregate metrics over 5 or 15 minutes, in some case 1 minute.
- This often hides:
  - Micro-bursts
  - Short-lived congestion
  - East-west traffic anomalies
- Critical performance issues disappear inside averaged data.

ntop

Predefined Constraints

- Traditional timeseries limit users to:
  - Metrics anticipated by developers
  - Static dashboard schemas
  - Fixed aggregation dimensions
- If a metric was not designed in advance, it cannot be analyzed later.

Flow-Based Observability

- ntopng now supports:
  - High-resolution counters for each raw network flow
  - 15-second timeseries generation
  - Near real-time visibility
  - Historical forensic analysis
- Key Concept
  - Every raw flow becomes an observability signal.
  - ➡ Any timeseries can be generated dynamically.

ntop

New Observability Use Cases

- Detect Micro-Bursts
  - Short spikes invisible in minute-based monitoring become immediately visible.
- Troubleshoot Intermittent Problems
  - Correlate: Packet spikes, Throughput changes, Traffic bursts, Application slowdowns
- Capacity Planning
  - Understand actual traffic dynamics instead of averages.

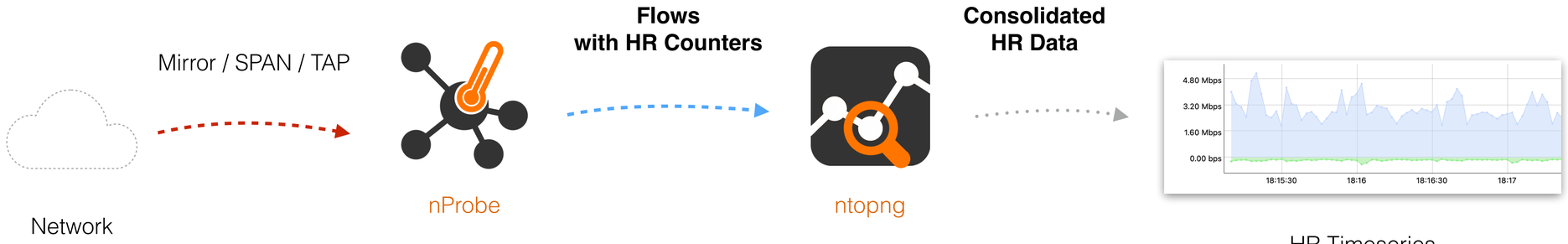
ntop

High-Resolution IEs

- nProbe as High-Resolution data producer
- New Information Elements with high-resolution timeseries, one per metric, including:
  - %HR_DST_TO_SRC_BYTES
  - %HR_SRC_TO_DST_BYTES

ntop

Data Pipeline



ntop

Examples of High-Resolution Analytics

- Build high-resolution timeseries on request, including:
  - Traffic between two hosts
  - Traffic toward an Autonomous System
  - Interface throughput
  - Per-application traffic
  - Per-country traffic
- Users can zoom from infrastructure-wide views down to individual flow behavior.

ntop

Unified Monitoring + Observability

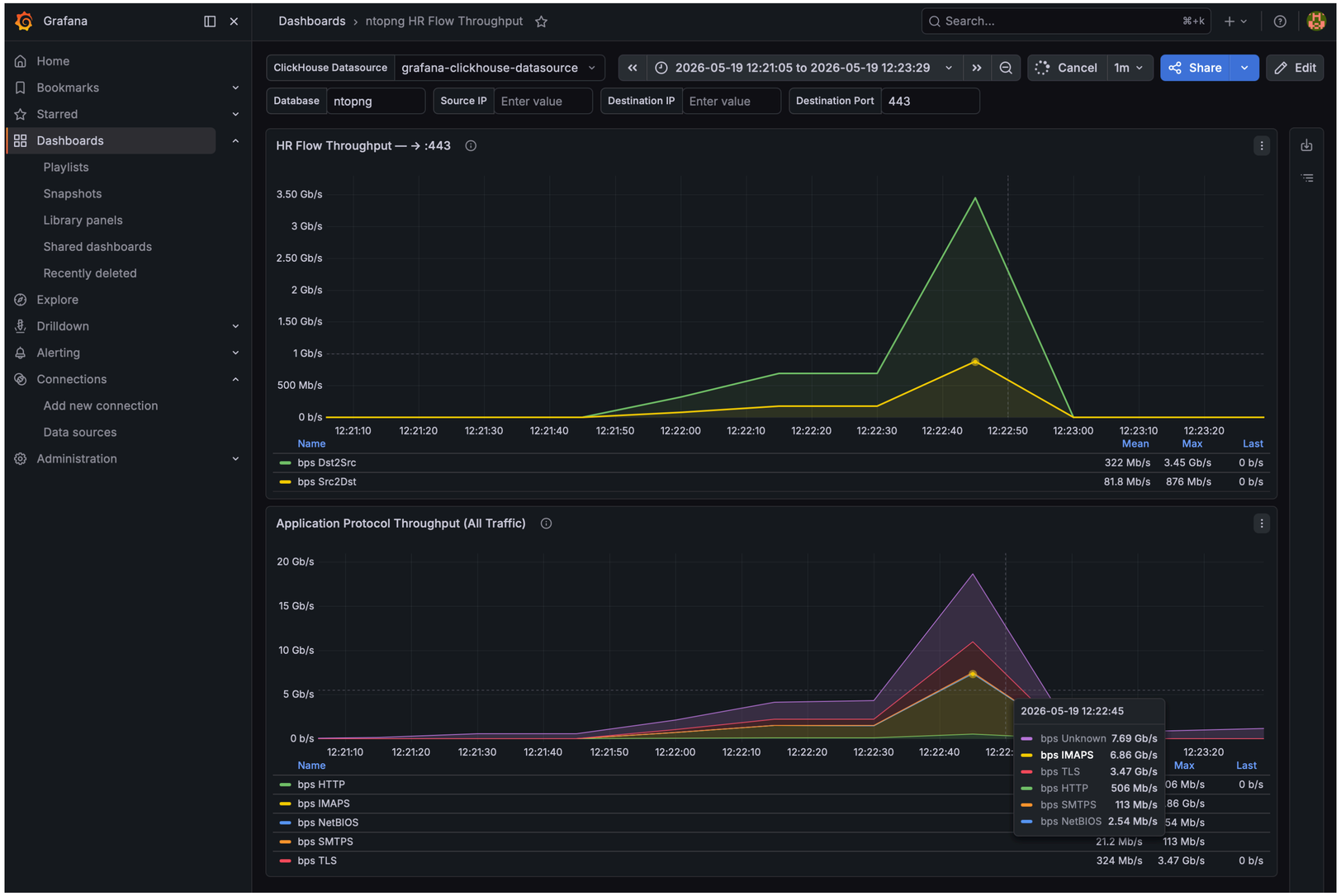
- ntopng now combines:
  - Traffic visibility
  - Security analytics
  - Historical analysis
  - Observability workflows
- Inside a single platform.

ntop

Chart HR Data in Grafana

ntop

Chart HR Data in Grafana



Webinar • May 21st, 2026

ntop

Future Directions

- The long-term vision is to evolve ntopng into a full observability platform.
  - Predictive anomaly detection
  - Automated incident detection
  - AI-assisted traffic analysis
- Goal
  - Transform network traffic into actionable operational intelligence.

ntop


thank you
danke
謝謝
merci
gracias
obrigado
dziękuję
teşekkür ederim
go raibh maith agat
ngiyabonga
спасибо
рахмат
Баярлалаа
bedankt
hvala
mauruuru
sukriya
kop khun krap
terima kasih
감사합니다
ευχαριστώ
arigatō
grazie
dakujem
merci
мерси
dank je
tapadh leat
mochchakkeram
sagolun
takk
tack
dhanyavadagalu
shukriya
diolch
xièxie
rahmat
rahmet
tanemirt
najis tuke
didi madloba
kam sah hamnida
ধন্যবাদ
chnorakaloutioun
gratias ago
gracies
sulpay
misaotra
matondo
blagodaram
vinaka
faafetai lava
kiitos
dankie
dhanyavad
gracie
bayarlalaa
enkosi
nandri
nanni
koszonom
akun
dankon
ačiū
djiere dieuf
tau
дякую
mamnun
chokrane
murakoze
tenki
obrigada
asante
manana
хвала
paldies
grazzi
mahalo
wetalin
barka
kia ora
mersi
spas
sobodi
dèkuji
mèsi
trugarez

ntop