NetBroker

powered by Combis

COMBIS NETWORK SOLUTIONS

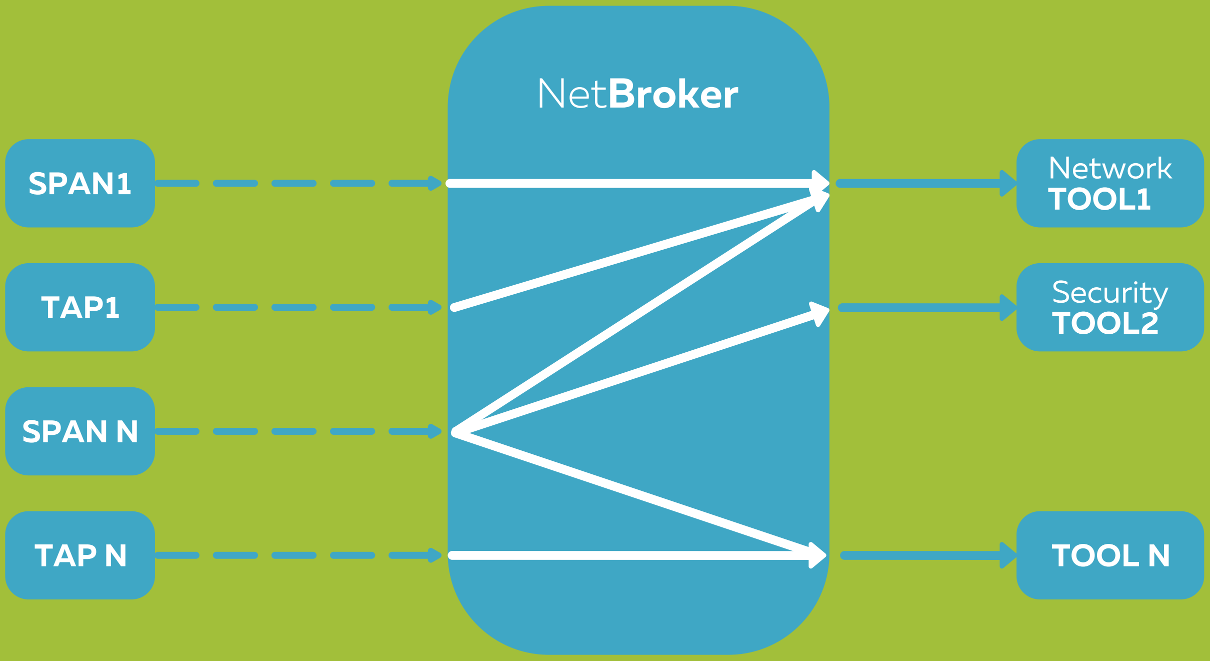
Modern networks demand modern approach

These days networks are getting more and more complex, especially if you add to it virtualized environments and cloud computing. Besides, security threats are becoming far more superior and sophisticated than ever before. That's where we come in! COMBIS has a response to all these challenges – our NetBroker is a next-generation network packet broker fabric that enables comprehensive end-to-end traffic visibility for different business needs mandated in modern network environments: network and security analytics, troubleshooting and many others.

What is **NetBroker**?

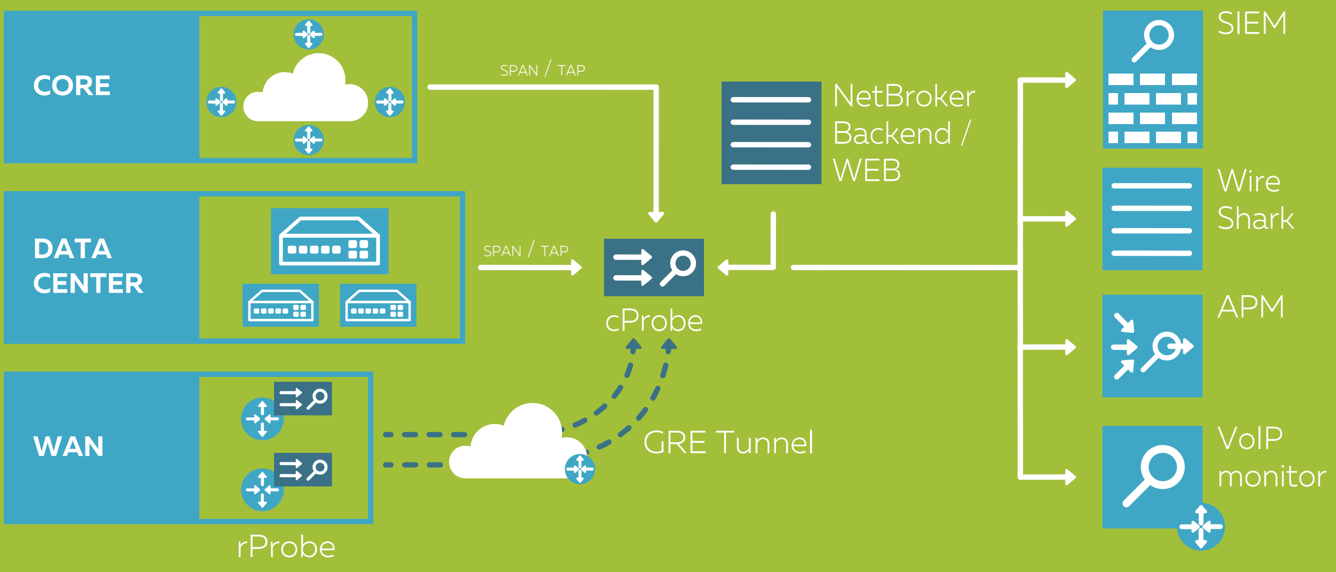
In a nutshell, Network Packet Broker is an out-of-band platform which takes input traffic from different sources (i.e. SPANs or taps), aggregates and filters traffic per programmed set of policy rules and steers traffic toward network tools to enable easily processing of this network traffic for better network analytics, troubleshooting and visibility purposes.

TRAFFIC AGGREGATION, FILTERING AND STEERING CONCEPT:



NetBroker acts as an overlay network fabric, having components distributed across whole network (WAN enterprise network, Virtualized datacenter, Telco core network). NetBroker probes can be distributed on remote location (i.e. other DC, POP, branch location) to locally aggregate, pre-filter traffic and steer traffic to a central location probe. A central probe can have multiple sources (SPAN, TAP, remote tunnel) which are cross-connected to multiple centralized networks & security tools. With this distributed architecture, NetBroker fabric provides true end-to-end traffic visibility across whole network.

GENERIC NETBROKER DEPLOYMENT MODEL:



Key Benefits for Customer

Network brokers try to solve following problems in networks, applications and security monitoring in Telco and Enterprise networks, which make the whole Time-to-resolve process slow:

- inability to see all traffic required by network tools - lack of centralized location to aggregate all traffic
- network tools inability of scale and high cost of supporting 10/40G networks – cost issues to maintain 1G tools to monitor 10G networks (or equivalent)
- troubleshooting processes too complex to perform on regular basis – joggling with scarce SPAN ports and having too many tools, missing granular filtering capabilities, etc.

WHEN DEPLOYED, NEBROKER BRINGS FOLLOWING BENEFITS:

Consolidation and optimization of monitoring/security tools – aggregating all network traffic and enabling shared access, one can centralize all monitoring tools to a single location. Instead of scaling network tools to match traffic growth, it is more cost effective to filter and deliver only relevant traffic, thus delivering significantly smaller amount of traffic and avoiding expensive tool upgrades.

Simple and quick deployment – NetBroker is essentially an out-of-band fabric and, by implementing approach "wire once and program per need", it will never impact production network.

Centralized management – enables agility in policy creation for filtering and delivering traffic to end tools. Once deployed, person requiring access to specific traffic can avoid cumbersome box-by-box reconfigurations in a network which is error prone, lacks scalability (SPAN restrictions), and granularity (on filtering level) through a centralized Web console.

Any-to-any connectivity – enables switching of packets from any input sources to any destination port where tools reside, overcoming SPAN/TAPs deficiencies like scarce resources and lack of filtering granularity.

Distributed architecture – traffic can also be processed on remote locations and delivered using overlay tunnels. There is no need to implement any specific changes in customer network to support distributed fabric functional end-to-end.

Automation – using external REST API enables automated tasks like creating and applying filters on the fly. I.e. IPS might generate a security alarm referring to a specific external IP address performing suspicious activities, SIEM can process an alarm and trigger API actions to NetBroker to start replicating specific flows toward the network recorder for further forensic activities.

Facilitated faster Time-to-resolution – especially valuable in complex networks and made possible by combining multiple NetBroker capabilities.

Traffic filtering and **steering capabilities**

NetBroker supports wide range of traffic filters for matching interesting traffic – ranging from L2 to L4 packet headers (to mention few like mac address, vlan, ip address, protocol). One can also filter by username, which is resolved in real-time by integrating with an identity service (i.e. Radius or Active Directory). Traffic can also be filtered per specific time of day and duration.

Complex filters can be built using many filter criteria and combining them using logical AND/OR operations.

NetBroker **Architecture**

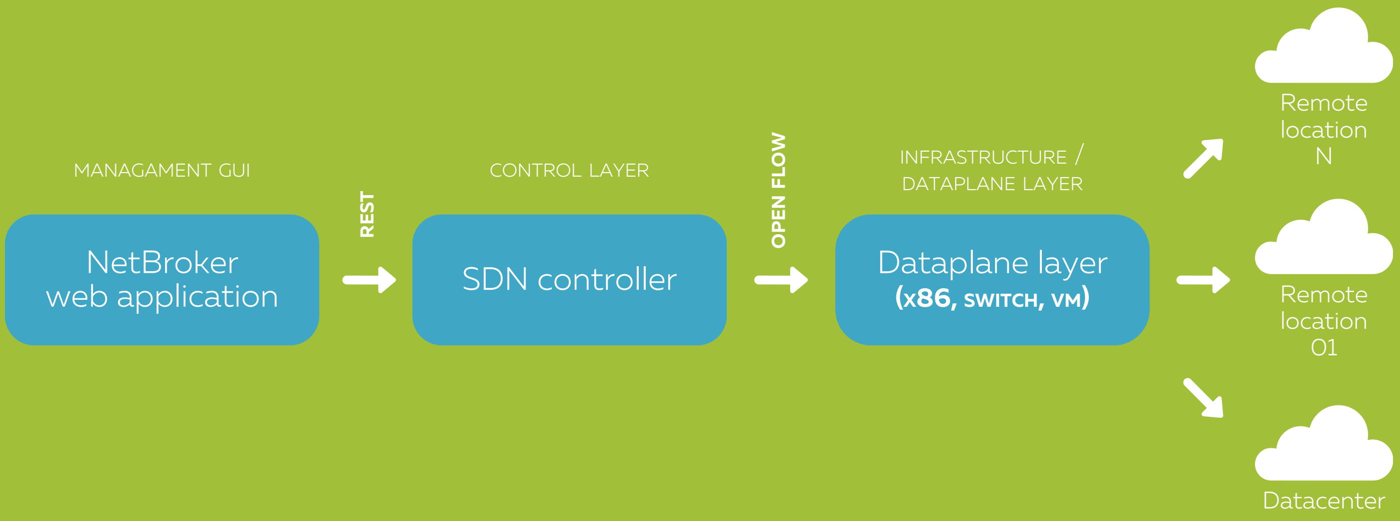
NetBroker is modular visibility fabric built on Software Defined networking (SDN) principles – centrally controlled & programmable, with separation of control and data plane.

NETBROKER CONSISTS OF MULTIPLE ELEMENTS:

Controller & Management plane and Web GUI is a customer facing component which is used to create network policies and distribute them across NetBroker elements.

NetBroker central data plane component aggregates all traffic, and performs policies for filtering and steering traffic to centralized network tool farms.

NetBroker remote data plane components can be distributed across remote locations to aggregate, pre-filter and route traffic to central locations using the overlay tunnel network (GRE – Generic Routing Encapsulation). Central aggregation component sees this tunneled traffic as another traffic source type (same way as local SPAN or TAP).



NetBroker **form factors**

Platform runs in many form factors, providing flexibility and best fit for the customer environment. Central components like controller and Web GUI, can be delivered either as virtual machines or on bare-metal servers.

Data plane software can run on many different form factors. Depending on customer's network, required throughputs, and deployment model, one can choose between: x86 server, high-speed network switch, virtual machine or Raspberry PI devices.

Who can **benefit the most**?

Any enterprise or telecom company that deals with complex network environments and needs to facilitate faster problem resolution as well as provide more secured environments.

Why **COMBIS**?

We develop and implement innovative solutions based on leading networking and communications technologies to provide you with advanced services, optimize your business processes and lower your operating costs. We analyze, design and implement contemporary solutions related to networking, datacenter, security and other advanced services. When it comes to our customers, we always strive to build strong partnerships and trust. Our priority is to go beyond and surpass expectations. This is COMBIS' definition of a job well done.

What next? **Contact us!**

For any additional information regarding network solutions please feel free to get back to us! Looking forward to hearing from you.

P: +385 1 3651 222 / E: sales@combis.eu / W: combis.eu