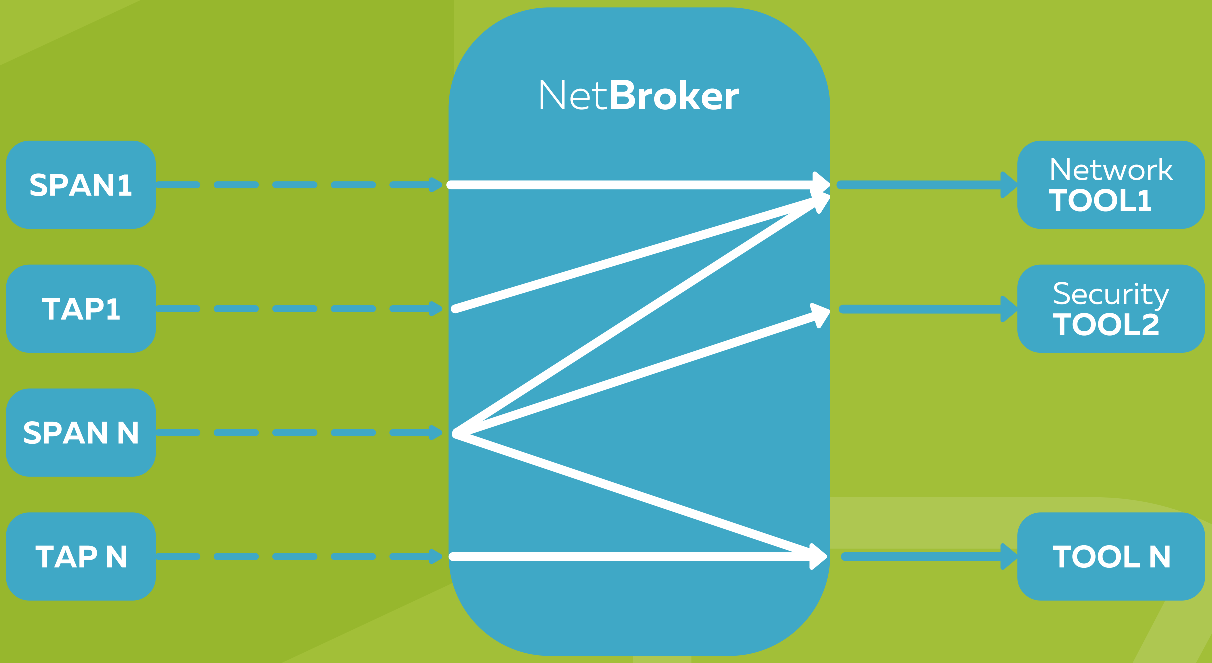
NetBroker

powered by Combis

What is NetBroker?

NetBroker is the next-generation Network Packet Broker (NPB), comprehensive end-to-end fabric, which enables network traffic aggregation and filtering to meet requirements in modern networks for network and security visibility, analytics and troubleshooting. NetBroker is an out-of-band platform that receives traffic from different network sources, like SPANs, TAPs, remote tunnels, and applies a set of policies to filter and deliver traffic to network tools.



Examples of Use Cases and Benefits

Centralized traffic visibility for all network tools - One can setup SPANs or taps only once, and then define all policies centrally as needed. Policies can be used both to aggregate, filter traffic and to route traffic to a required destination (i.e. analysis & monitoring tools, network recorders, security tools, etc.).

Optimize monitoring tools costs – Instead of investing in a monitoring tools upgrade, due to traffic increase, one can centrally filter and deliver only a subset of relevant traffic to network tools. This delivers a significantly smaller amount of traffic, thus lowering costs of investment.

Security analysis – Security tools need to see all traffic for multiple purposes (traffic replay/analysis, network recording for security sensible traffic) and have to be able to automate the capture of traffic for forensics purposes. Tools like SIEMs, IDS, APT/ATP can enhance scalability, functionality, and capacity if only receiving business related traffic.

Platform Features and Benefits

DISTRIBUTED ARCHITECTURE

- Probes can be distributed to hundreds of locations.
  Control and data plane separation – policy & control components can reside separately in customer datacenter.

WEB GUI

- Moderm Web GUI for centralized policy creation.

AUTOMATION

- Automate filter creation using platform REST API. Different tools (i.e. SIEM) can automate actions to process traffic in network according to some event.

SECURITY RBAC MODEL

- Basic security RBAC model is provided to allow the administrator to grant a user permission to see and deliver network traffic to destination tool.

OPENNESS

- Platform built on SDN paradigm, enable quick feature development.

Filtering and Steering Capabilities

TRAFFIC FILTERING AND STEERING PROVIDE MANY CAPABILITIES TO ENABLE FLEXIBLE AND EASY TRAFFIC OPERATIONS.

L2 – L4 FILTERING CAPABILITIES

- L2 filters: match on source/destination mac addresses, VLAN tags.
- L3 – IP source/destination, protocols (TCP, UDP, ICMP, GRE, SCTP etc.).
- L4 – TCP, UDP source/destination ports to identify applications.

PROTOCOLS

- Supported both IPv4 and IPv6 protocols.

FILTER PER USERNAME

- Connect to identity services to support filtering per usernames (resolve user-to-ip mapping in realtime).
- Radius and Active Directory identity services supported.

PER SPECIFIC TIME

- Traffic can be filtered per specific timeframe.

LOCATION BASED

- When automating filter, filter will be applied to closest NetBroker unit in network for optimization purposes.

COMPLEX OPERATIONS

- Capability to construct complex filters by using many filter conditions and combining them by using logical AND/OR operations.

FLEXIBLE TRAFFIC DELIVERING TO NETWORK & SECURITY TOOLS	→ N-to-M model - multiple input sources (SPANs, TAPs) are aggregated, multiple filters applied and forwarded to multiple destination ports. → Remote probe can pre-filter traffic on remote location and backhaul it over customer IP network to central location where traffic can be additionally filtered and forwarded to multiple locations.
TRAFFIC DISTRIBUTION / LOAD BALANCING	→ Load balance traffic to multiple tools defining policy how to distribute flows to tools to scale monitoring and enable high availability.
NETFLOW / IPFIX *	→ Generate Netflow (v5, v9) or IPFIX records for traffic traversing NetBroker.
PACKET MANIPULATION *	→ Prior to being delivered to network tools, packet payload can be truncated to enable privacy protection and better network tool scaling.

*** Depends on hw platform. Some platforms don't support packet manipulations.**

Supported **Form-Factors**

DIFFERENT FORM FACTORS ARE SUPPORTED TO PROVIDE SCALABILITY WITH BEST PRICE PERFORMANCE.

X86 SERVER	→ Runs on x86 COTS server. → Good for moderate size environments up to several 10Gbps aggregated traffic with few traffic sources.
NETWORK SWITCH	→ Runs on network switch with multiple 1G/10G/40G physical ports. → Model is fit for larger enterprise and Service Provider networks, where multiple high-speed input and output ports are required (i.e. 10Gbps and 40Gbps ports).
VIRTUAL MACHINE *	→ Delivers traffic flowing between VMs in virtual environments. → Supports different virtualization platforms – VMWare ESXi, Microsoft Hyper-V, KVM, Citrix Xen.
RASPBERRY PI	→ Provides cost effective remote probe to pre-filter required traffic and sends traffic to a central location by using Tunnel overlay technologies.

*** Deployment model depends on virtualization architecture and needs to be designed and verified according to customer environment.**

Want to know **more?**

For any additional information 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