TAPPING INTO VIRTUAL ENVIRONMETS

Netzwerk-Monitoring ist essentiell wichtig
um sich vor **Bedrohungen** zu schützen
und **Performance** zu gewährleisten!

Aber **wie** kann ich meine virtuellen und
Cloud-Umgebungen ausreichend **überwachen**

PacketRavenVirtual – 100% Network Access in Physical, Virtual Environments & Cloud

Mit dem neuen NEOX Virtual Netzwerk-TAP

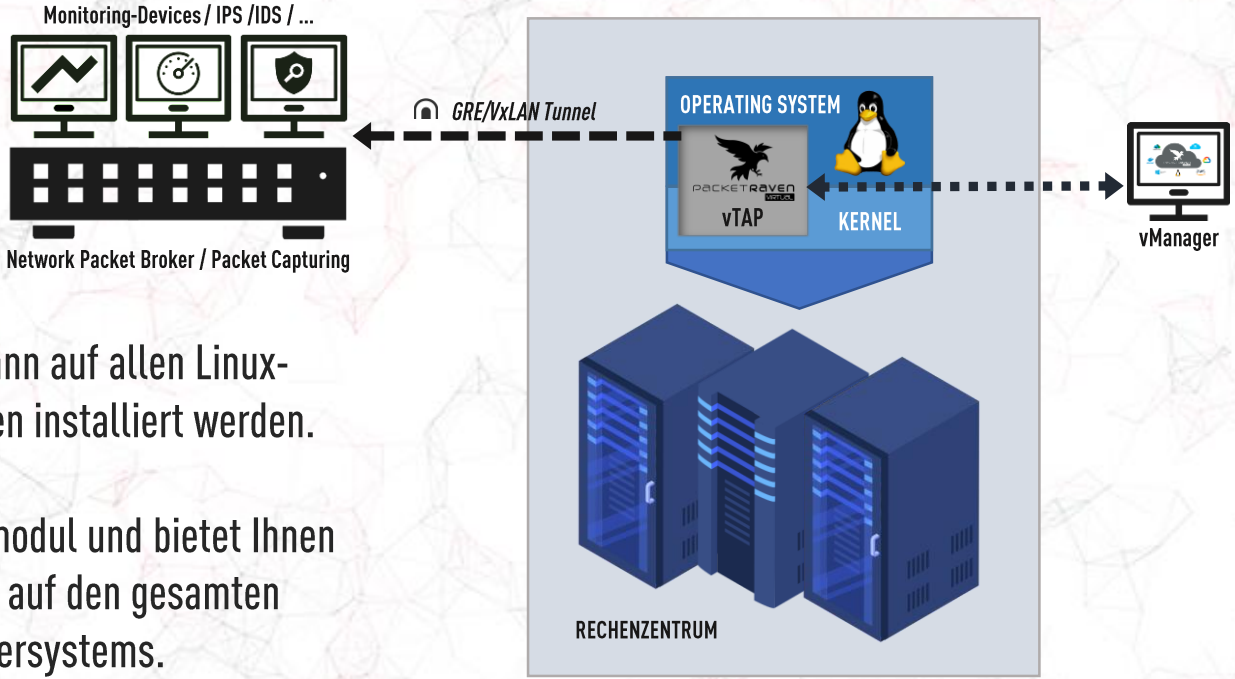
- Verfügbar für verschiedene Umgebungen: Azure Cloud, Google Cloud, AWS, VMware, Dedicated Server, etc.
- Keine Begrenzung durch die Netzwerkgeschwindigkeit
- Zuverlässigere Alternative zur virtuellen Port-Spiegelung
- Stateful-Filtering (verbindungsorientierte Filterung)
- Mehrere GRE/VxLAN-Tunnel
- Unterstützt die Modi Aggregation und Regeneration (n:1 und 1:n)
- Einfach zu installieren (Debian-Paket oder Docker-Image) und intuitiv zu konfigurieren
- Programmiert, entwickelt und getestet in Deutschland

- Volle Netzwerktransparenz
- Keine Beeinträchtigung des Datenverkehrs
- 100% Netzwerkdaten
- Für verschiedene Umgebungen
- Uneingeschränkte Netzwerkgeschwindigkeit
- Flexibel einsetzbar
- Alternative zum virtuellen Port-Mirroring
- Einfach zu installieren & konfigurieren
- GRE/VxLAN Tunnel
- OSI Layer 2-4 Stateful Filtering
- Aggregation n:1
- Regeneration/Replication 1:n
- Entwickelt & programmiert in Deutschland

EINSATZSZENARIEN

Physisch, Virtuell, Cloud

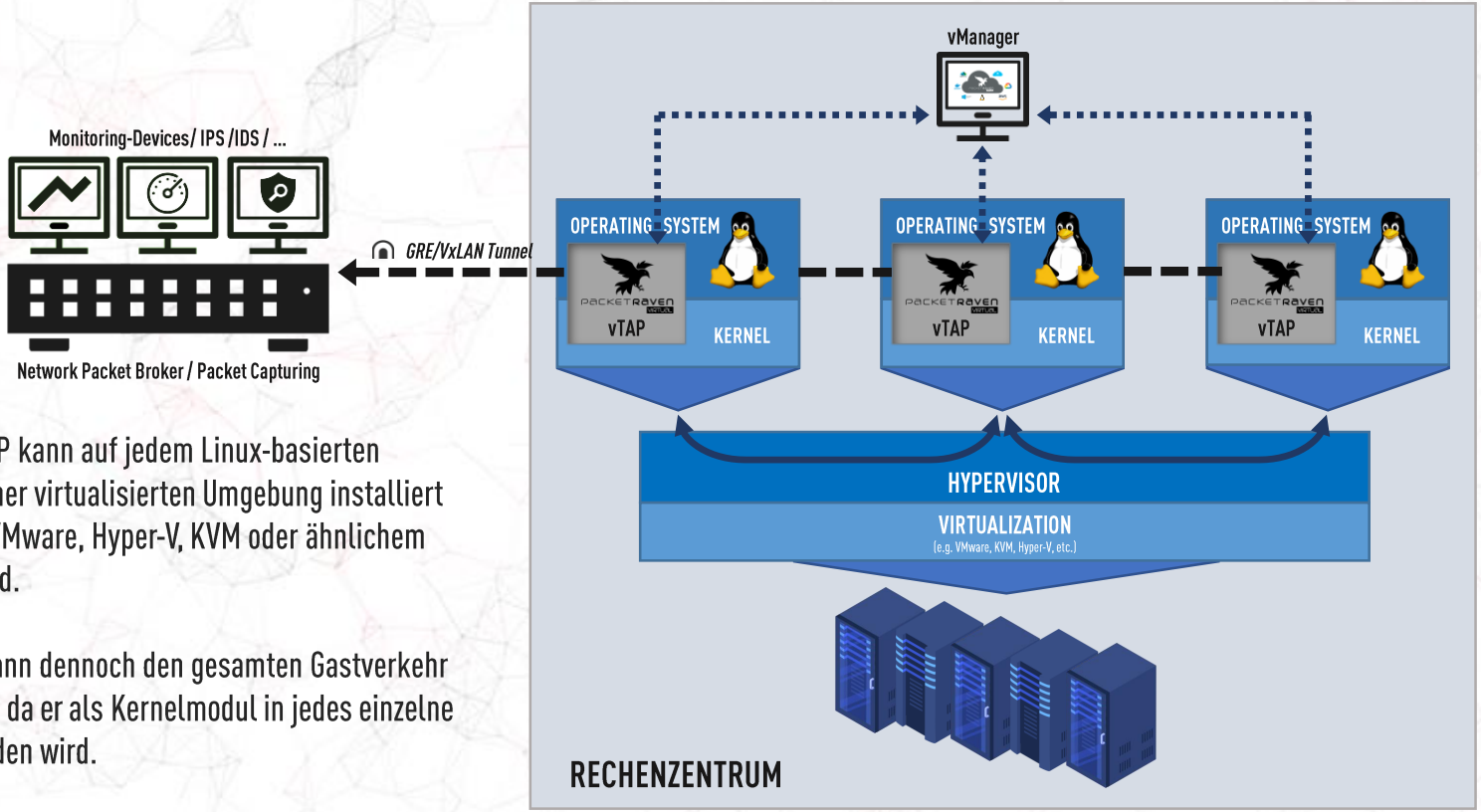
EINSATZSZENARIO I.: PHYSISCH | LINUX OS



NEOXPacketRaven vTAP kann auf allen Linux-basierten Betriebssystemen installiert werden.

NEOX' vTAP ist ein Kernelmodul und bietet Ihnen vollen Zugriff/Sichtbarkeit auf den gesamten Netzwerkverkehr des Serversystems.

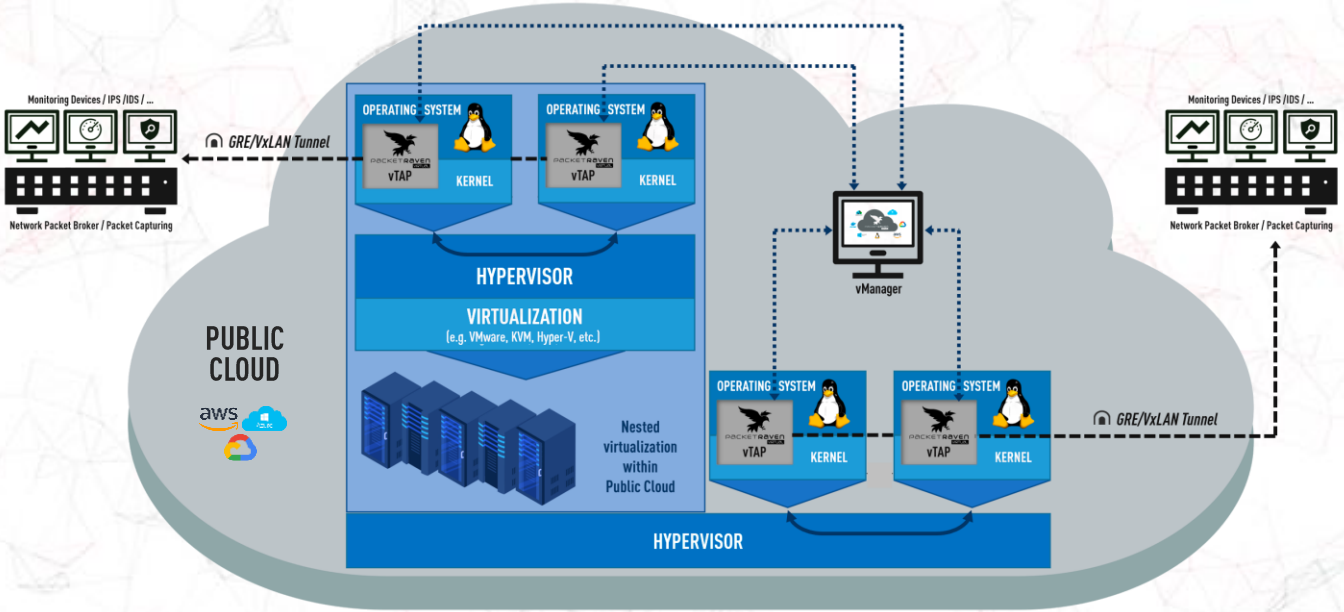
EINSATZSZENARIO II.: VIRTUELLE UMGEBUNGEN



PacketRaven vTAP kann auf jedem Linux-basierten Gastsystem in einer virtualisierten Umgebung installiert werden, die von VMware, Hyper-V, KVM oder ähnlichem bereitgestellt wird.

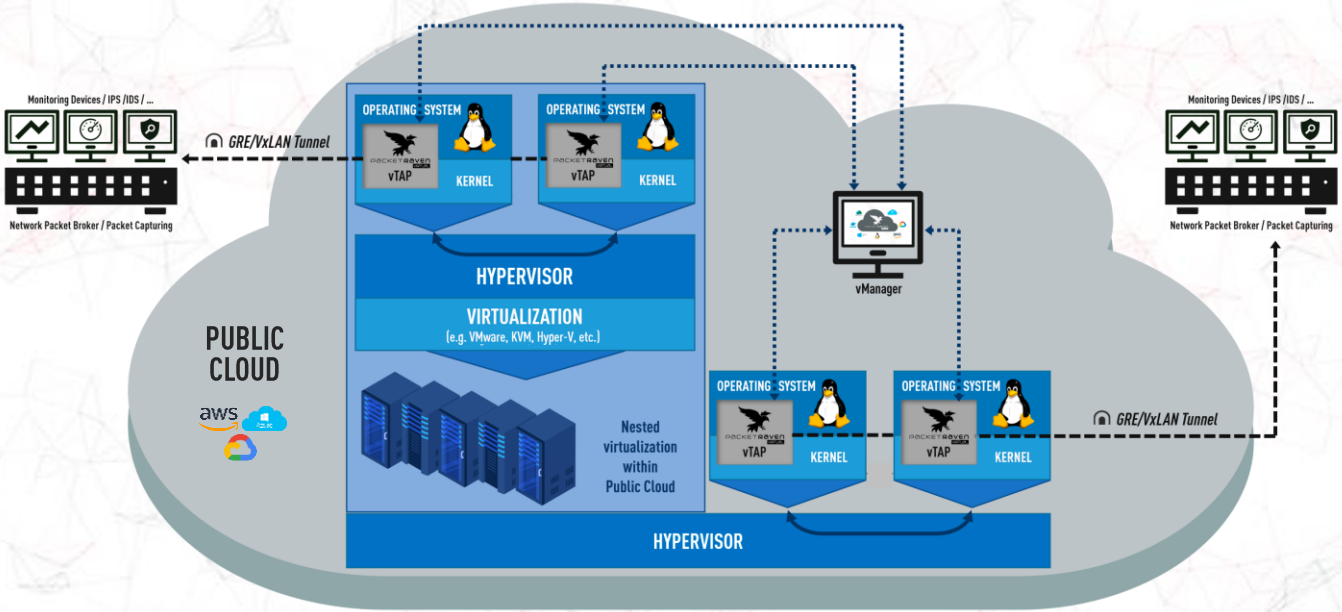
Der NEOX vTAP kann dennoch den gesamten Gastverkehr sichtbar machen, da er als Kernelmodul in jedes einzelne Gastsystem geladen wird.

EINSATZSZENARIO III.: CLOUD-UMGEBUNGEN



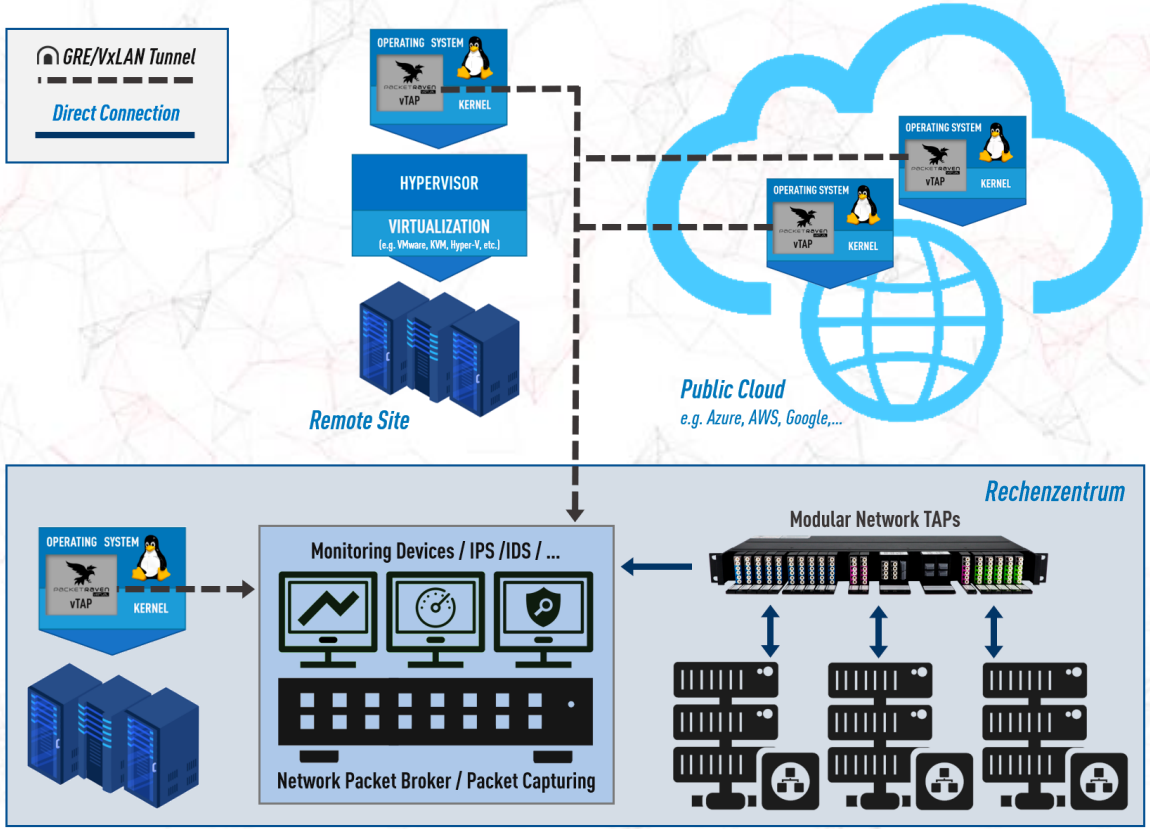
Da häufigere Installationen von NEOX vTAP vollständig unterstützt werden, da ein Kernelmodul verwendet wird, anstatt in den Hypervisor selbst einzugreifen, stellt auch eine verschachtelte Virtualisierung wie die oben beschriebene kein Hindernis für NEOX vTAP dar. Sie spiegelt den gesamten Datenverkehr direkt aus dem Linux-Kernel des jeweiligen Gastsystems und sendet den Verkehr per gekapseltem Tunnel wie VxLAN oder GRE aus.

EINSATZSZENARIO III.: CLOUD-UMGEBUNGEN



Since more common installations are fully supported by the NEOX vTAP due to approach of using a kernel module instead of trying to interfere with the hypervisor itself,
even a nested virtualization setup like the one above shows no obstacles for the NEOX vTAP. It mirrors the entire traffic directly from the Linux kernel of each guest system and sends the traffic out per encapsulated tunnel such as VxLAN or GRE.

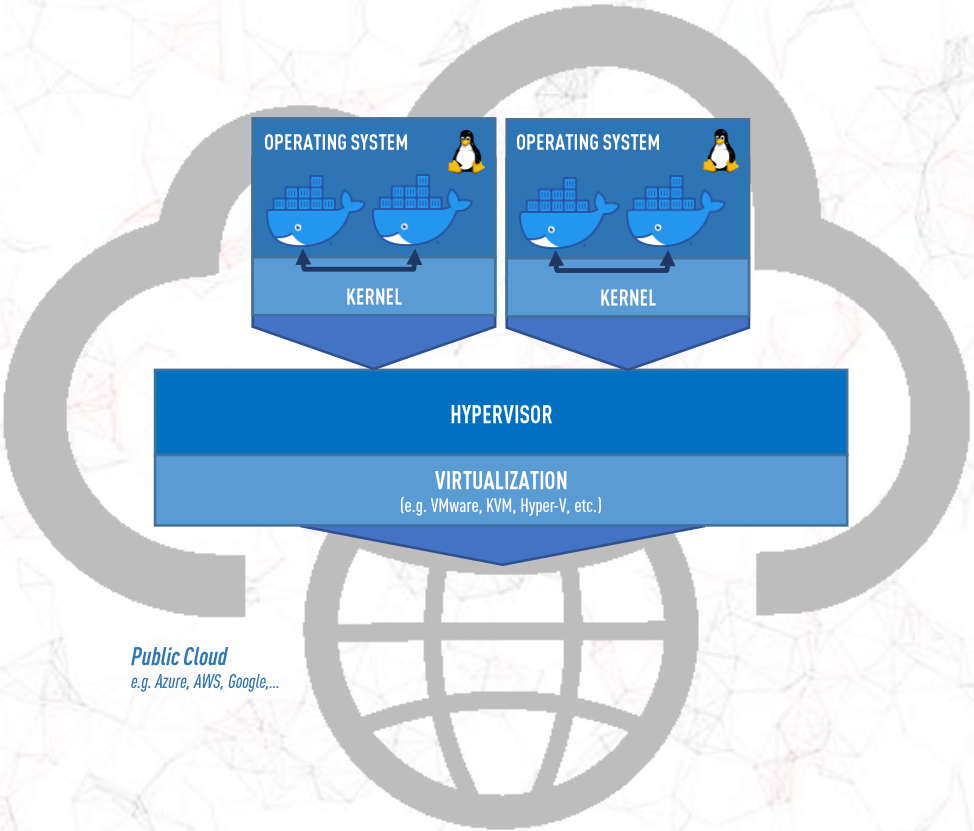
EINSATZSZENARIO : PHYSISCH | VIRTUELL | CLOUD



EINSATZSZENARIEN

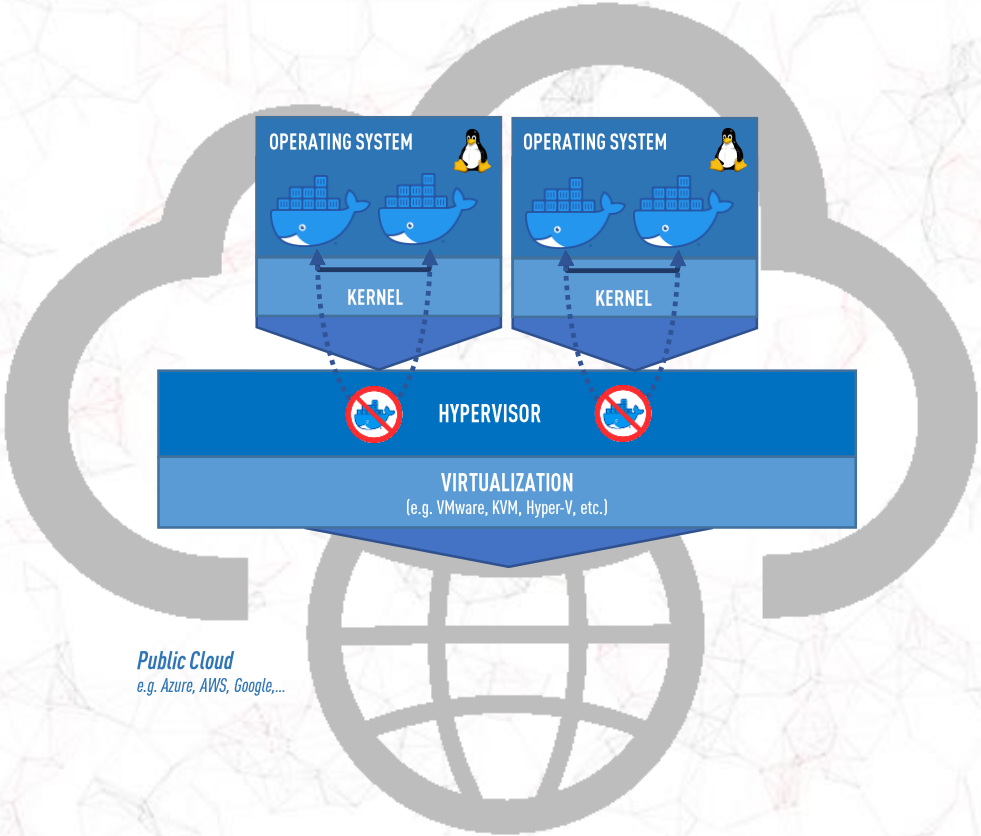
Monitoring von DOCKER Netzwerkverkehr

EINSATZSZENARIO: MONITORING DOCKER TRAFFIC – HERAUSFORDERUNG I.



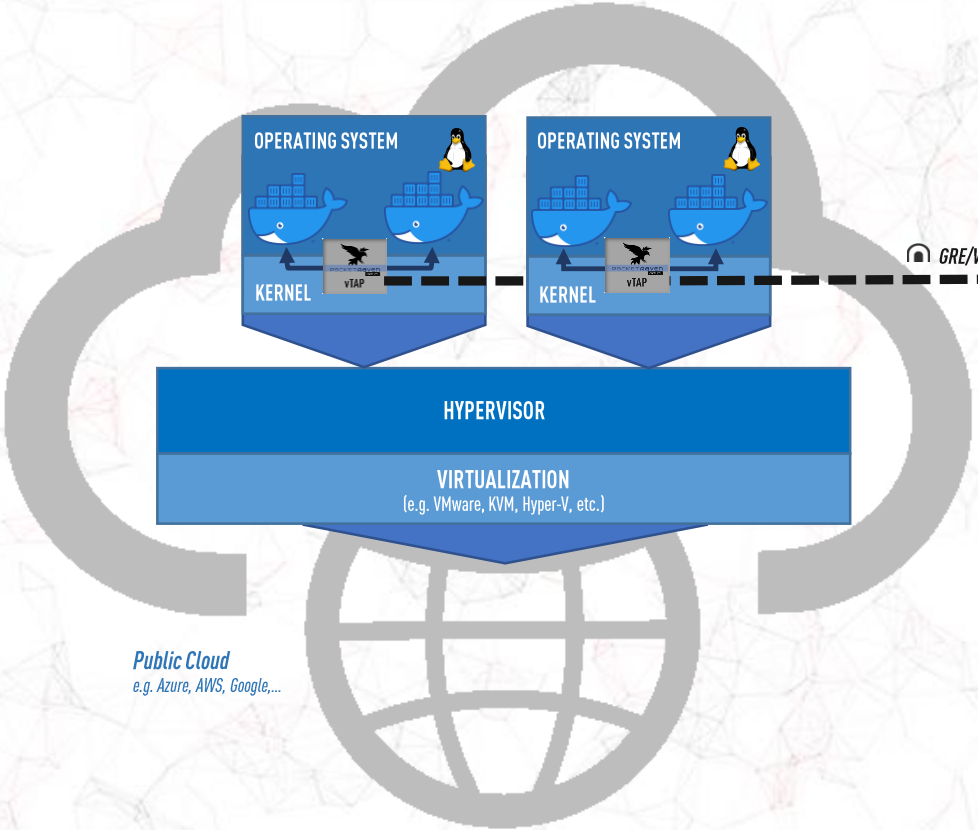
PROBLEM:
Der Datenverkehr zwischen Docker-Containern geht **nicht** an den Hypervisor und bleibt nur auf dem Host!

EINSATZSZENARIO: MONITORING DOCKER TRAFFIC – HERAUSFORDERUNG II.



PROBLEM:
Durch Spiegeln oder Abgreifen des Hypervisors können Sie den kritischen Inter-Docker-Verkehr **nicht sehen.**

EINSATZSZENARIO: MONITORING DOCKER TRAFFIC – LÖSUNG



LÖSUNG:

NEOXPacketRaven vTAP unterstützt das abgreifen des „inner-guest“/ “inter-Docker“/ “inner-container“ Netzwerkverkehrs.

Mit NEOX vTAP

FAZIT

FAZIT

ANWENDUNGSFÄLLE

- Erhalten Sie 100%ige Cloud-Netzwerkdaten für die Analyse und Fehlersuche
- Verstärkung der Sicherheitsabwehr
- Verringerung von Performance-Problemen
- Konsolidierung von Initiativen zur Einhaltung von Vorschriften

VORTEILE GEGENÜBER DEM VIRTUELLEN PORT-MIRRORING

- Eine granularere Aufteilung, z. B. n:1 (Aggregation) oder 1:n (Regeneration) ist möglich.
- Spiegeln Sie den Verkehr pro Richtung, z. B. den eingehenden, den ausgehenden oder den gesamten Netzwerkverkehr.
- Verbindung zu physischen Geräten über GRE/VxLAN-Tunneling, was bei Port-Mirroring nahezu unmöglich ist.
- Stateful-Filtering, um nur relevante Daten zu kopieren und angeschlossene Tools zu entlasten
- Cloud-Anbieter können die Port-Spiegelung gemäß ihren Bedingungen einschränken.

DANKE FÜR IHR INTERESSE

TRANSPARENZ

das Fundament für Ihre Netzwerksicherheit

NEOX NETWORKS GmbH
Monzastr. 4
63225 Langen
Deutschland

T: +49 6103 37 215-910

solutions@neox-networks.com

www.neox-networks.com