

NEOXPacketTigerVirtual

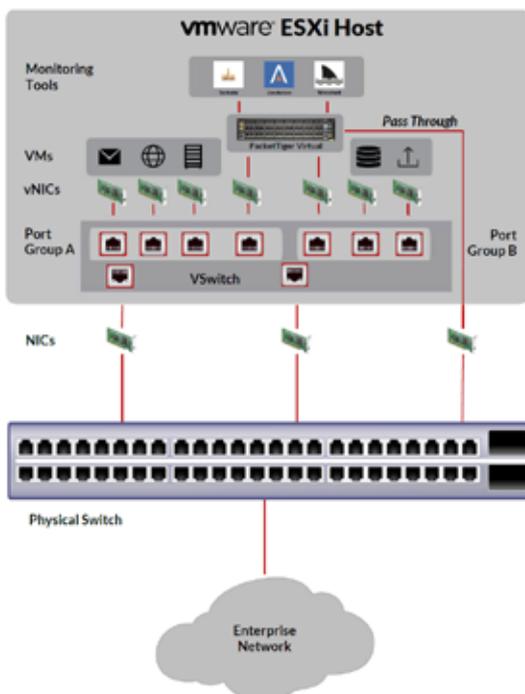
MAXIMIEREN SIE DIE NETZWERKSICHTBARKEIT MIT UNSERER INNOVATIVEN VIRTUELLEN NEXT-GEN PACKET-BROKER-PLATTFORM!



Mit unserer Network Packet Broker Produktfamilie NEOXPacketTiger gehen Sie keine Kompromisse bei der Sicherheit, Leistung und Ende-zu-Ende-Servicequalität ein. Die heutige Netzwerk-Infrastruktur muss vieles leisten, dabei 24x7 unterbrechungsfrei funktionieren und stellt kritischen Applikationen die notwendigen Datenverbindungen zur Verfügung. Die Vorteile von virtuellen Rechenzentren, Cloud-Lösungen und SD-WAN-Technologien liegen auf der Hand. Aufgrund höherer Komplexität der Kommunikationswege fehlt Ihnen oft die Transparenz sowohl in physischen als auch virtuellen Netzwerken. Aber genau ohne diese Sichtbarkeit bzw. Transparenz können Bedrohungen unentdeckt bleiben und verringern die Leistung Ihrer Security- und Monitoring Tools.

Die vermehrte Verschiebung von physischen Systemen zu virtuellen und hybriden Umgebungen stellt Netzwerk-Managern vor noch nie dagewesene Herausforderungen, wenn es um die Leistungsgüte und die Unternehmenssicherheit geht. Aufgrund dieser Migration in die Cloud und virtuelle Umgebungen verlieren Ihre bestehenden physischen Monitoring-, Analyse- und Security-Tools den Zugriff auf Ihren kritischen Netzwerkverkehr, was zu einer weiteren Verschlechterung der Sichtbarkeit führt. Hinzu kommt, dass neue Lösungen derzeit in virtueller Form bereitgestellt werden, womit eine weitere Herausforderung an die Netzwerk-Infrastruktur gestellt wird.

Mit dem NEOXPacketTiger stellen wir Ihnen eine Network-Packet-Broker-Lösung zur Verfügung, um den Anforderungen an mehr Sichtbarkeit und Transparenz in sowohl physischen als auch virtuellen Netzwerkumgebungen gerecht zu werden. Somit erhalten SecOps und auch NetOps die umfangreichen als auch notwendigen Funktionen eines hybriden Network Packet Brokers, die Sie für Ihre Security- und Monitoring-Tools benötigen.



KEY FEATURES

GTP Correlation + GTP inner IP Load Balancing + IMSI Filtering

Verbindet mit physischen und virtuellen NICs

Virtuelle Umgebungen: ESXi, OpenStack, Docker Container

Einheitliche Netzwerktransparenz über virtuelle und physische Netzwerke hinweg

Mehrere Management-Optionen (CLI, SSH, SNMP V2/V3, WEB UI, Net CONF und REST API)

Administrierbar mittels NEOXPacketDirector

APPLICATION AREAS

Bereitstellung von Netzwerktransparenz für virtuellen Netzwerkverkehr

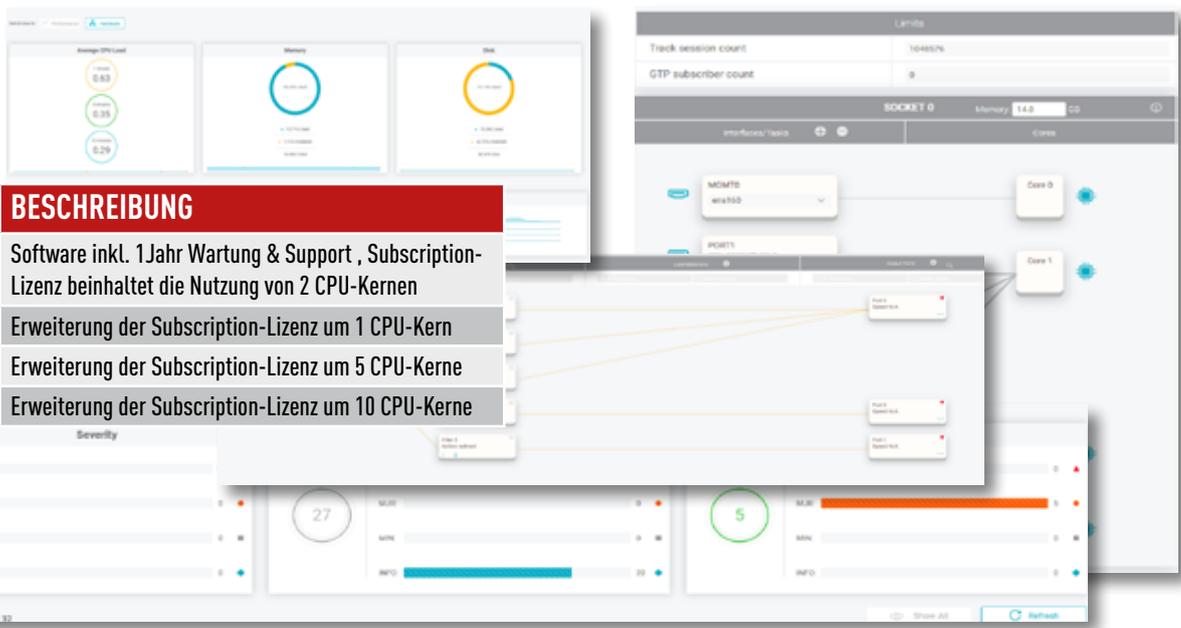
Umleitung von virtuellem Netzwerkverkehr an Monitoring-Tools in physischen und/oder virtuellen Umgebungen

Nutzung von physischen Monitoring-Tools bei der Migration zu virtuellen Umgebungen

Optimieren Sie virtuelle und physische Monitoring-Tools durch das Filtern von Daten

Gleichgewicht zwischen physischen und virtuellen Monitoring-Tools

| FEATURES | BENEFITS |
|----------------------------|---|
| Aggregation | Aggregieren und Umleiten von Netzwerkverkehr zur weiteren Verarbeitung |
| Replication | Mehrere Tools zur Analyse desselben Datenverkehrs zulassen |
| Inner Tunnel Filtering | Filterung nach inneren Tunnelparametern (GTP, VXLAN, L2TP) |
| GRE Tunneling | Zusammenschaltung von Packet Brokern über mehrere Standorte mittels L3GRE- & NVGRE-Protokoll |
| Filtering | Herausfiltern von unnötigem Netzwerkverkehr mit bedingten 5-Tupel-Klassifikatoren |
| User Defined Filters (UDF) | Pakete verfolgen, die mit einem bestimmten „Window“ im eingehenden Verkehr übereinstimmen |
| AND/OR/NOT Operatoren | Vereinfachen Sie den Betrieb des Packet Brokers mit logischen Filteraktionen |
| Copy | Aktivieren Sie orthogonale Filterpfade für denselben Netzwerkverkehr |
| Layer-7 Filtering | DPI durchführen und Tausende von Layer-7-Protokollen identifizieren |
| Regex Filtering | Identifizierung und Filterung von Datenverkehr (stream- oder paketbasiert), der bestimmte Zeichenfolgen enthält |
| Weighted Load Balancing | Verteilen Sie den Datenverkehr auf mehrere Tools und verhindern Sie eine Überbelegung |
| Session Tracking | Verfolgen Sie die gesamte Sitzung, sobald das gewünschte Muster identifiziert wurde |
| Port Labelling | Verfolgen Sie den Paketpfad durch Hinzufügen von VLAN-Tags, die den Eingangsport angeben |
| Header Stripping | Header entfernen (MPLS, VLAN, PPP, QinQ, VN-TAG, VXLAN, GRE, GTP, L2TP, Geneve) |
| Header Editing | Modifizieren von MAC-, VLAN- and IP-Headern |
| Deduplication | Maximierung der Tool-Leistung durch Eliminierung doppelter Pakete |
| Data Masking | Schützen Sie sensible Daten, indem Sie diese überschreiben, bevor sie an die Tools gesendet werden |
| Packet Slicing | Reduzieren der Datenüberlastung durch Entfernen der Paketnutzlast und/oder aller unnötigen Daten |
| Meta-data Extraction | Erzeugen von Metadaten für Syslog- oder Kafka-Server |
| Capping & Sampling | Reduzieren Sie den Datenverkehr durch Stichproben und/oder Begrenzung der Raten |
| Time Stamping | Verbessert die Netzwerktopologie durch Timestamping im Nanosekundenbereich |
| Capture & Replay | Erfassen von PCAP-Dateien in Filtergranularität und Wiedergabe zur weiteren Analyse |
| De-Fragmentation | Zusammensetzen von Paketfragmenten zu vollständigen Paketen |
| IPFIX/NetFlow | Generierung und Verteilung von IPFIX/NetFlow Flows |
| Management | Web UI, SSH, CLI, SNMP, Net CONF, REST API |



| ART. NR. | BESCHREIBUNG |
|-------------|--|
| NX-PBPT-VM | Software inkl. 1Jahr Wartung & Support , Subscription-Lizenz beinhaltet die Nutzung von 2 CPU-Kernen |
| NX-PBPT-L1 | Erweiterung der Subscription-Lizenz um 1 CPU-Kern |
| NX-PBPT-L5 | Erweiterung der Subscription-Lizenz um 5 CPU-Kerne |
| NX-PBPT-L10 | Erweiterung der Subscription-Lizenz um 10 CPU-Kerne |

Rev. 1.1 / 04.02.2025