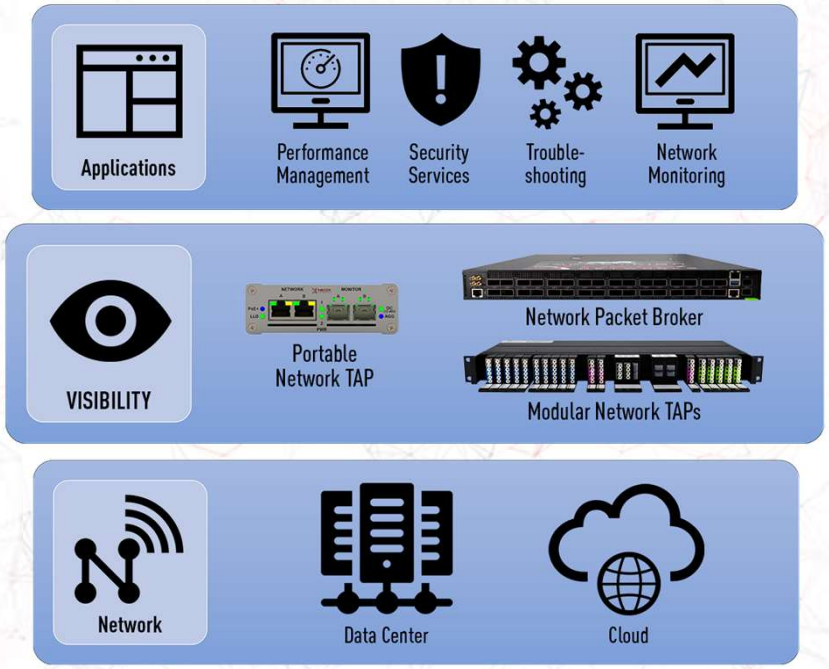
Netzwerksicherheit im toten Winkel
360 Grad Rundumsicht dank Netzwerk-TAPs

Dienstag, 25.10.2022
10:30 h - Forum D, Halle 7

Wo befindet sich eigentlich die Visibility-Ebene?



- Die Visibility- oder auch Transparenz-Ebene ist ein Geflecht, welches aus Geräten besteht, die Sicherheits-, Überwachungs- und Netzwerk-Performance-Appliances miteinander verbinden.

- Es ermöglicht das Senden von ausgeleitetem Datenverkehr an die gewünschten Ziele und die Festlegung von Maßnahmen bei Ausfällen von Verbindungs- oder Sicherheitsgeräten oder bei Angriffsszenarien.

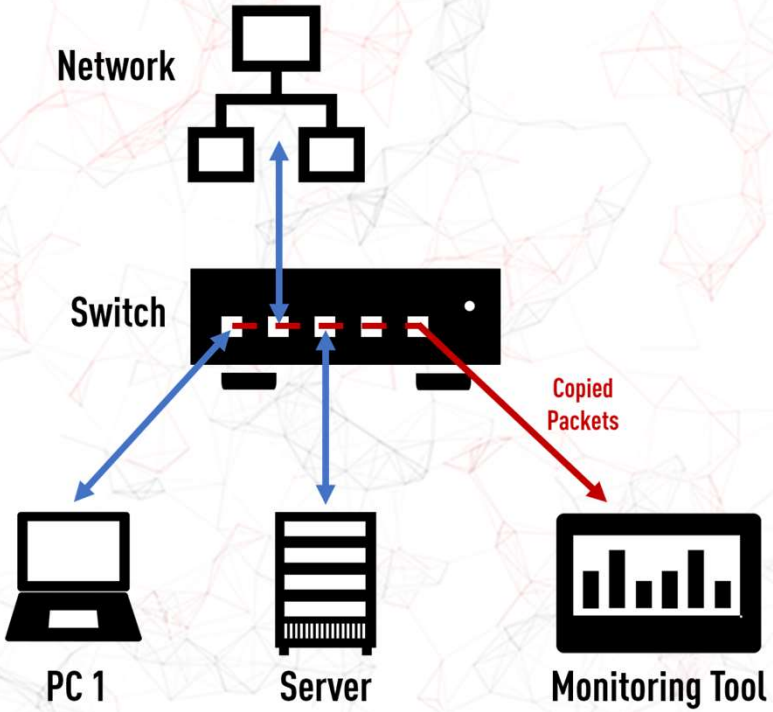
6 gute Gründe, warum Sie Transparenz benötigen

- Detaillierte Überwachung des Netzwerkverkehrs auf bösartiges Verhalten und potenzielle Bedrohungen hin
- Optimieren der Performance des Netzwerks und der Applikationen
- Erhöhtes Bewusstsein für das Verhalten des Netzwerkverkehrs
- Grundlage für ein gesundes Netzwerk zur Verbesserung von Effizienz, Sicherheit und Performance
- Ermöglicht die Hervorhebung von Sicherheitsrisiken, um entsprechende Abhilfemaßnahmen zu priorisieren und anzuwenden
- Mehr Kontrolle über Netzwerke und bessere Entscheidungsmöglichkeiten in Bezug auf Datenschutz und Datenfluss

TOP 5 - Warum entstehen Transparenzprobleme?

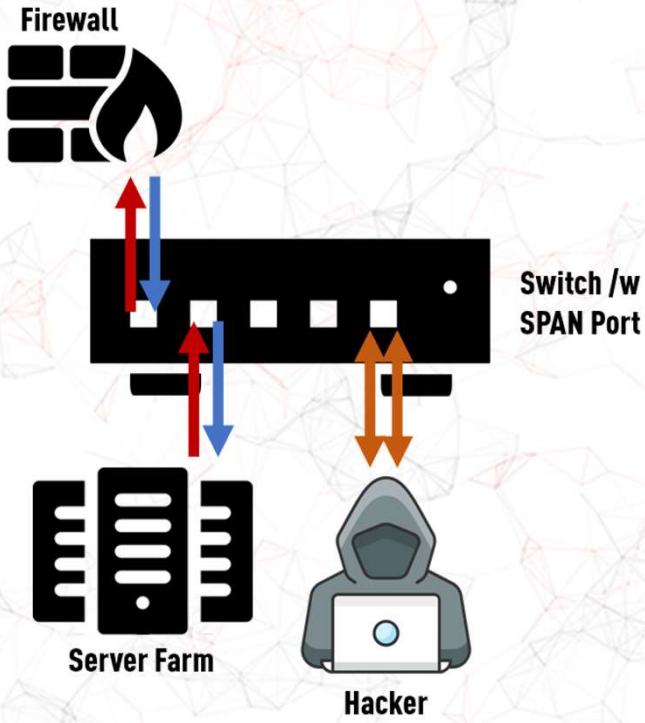
Blinde Flecken aufdecken	Kapazitätsplanung	Diskrepanz zwischen Werkzeugen und Netzwerk-kapazität	Verwaltung entfernter Standorte	Beseitigung von Netzwerk-konflikten (SPAN & abteilungs-spezifische Limitierungen)

Was ist ein SPAN-Port bzw. Port-Mirroring?



Beim Port-Mirroring werden die benötigten Netzwerkdaten mittels einer Spiegelung der Switch-Ports zur Verfügung gestellt.

Die 9 grössten Nachteile des Port-Mirrorings



Die Verwendung eines SPAN-Ports hat aber mehrere Nachteile:

- Paketverluste können auftreten
- Paketreihenfolge kann verfälscht werden
- Paketduplikate können entstehen
- Der Switch ist ein aktives Gerät und kann angegriffen werden
- Verursacht zusätzliche Latenzzeit
- CRC/FCS fehlerhafte Pakete werden nicht gespiegelt
- Unterstützt keine Vollduplex-Verkehrsanalyse
- Kann leicht überbucht werden
- Microbursts werden möglicherweise nicht weitergeleitet

Was ist ein Netzwerk-TAP?

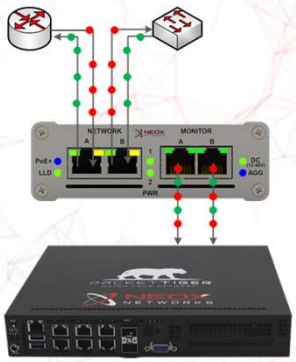
- Der Ausdruck TAP ist eine Abkürzung und steht für TEST ACCESS PORT
- Ein Netzwerk-TAP, auch Ethernet-TAP genannt, stellt einen passiven Zugriffspunkt zu einer Netzwerkverbindung her, womit die über das Kabel übertragenen Datensignale zu Analysezwecken mitgelesen und ausgewertet werden können
- Kann den gesamten Datenverkehr transparent, schnell, einfach und ohne Beeinträchtigung der aktiven Netzwerkleitung, für verschiedenste Monitoring-Anwendungen bereitstellen.
- Arbeitet auf dem OSI Layer 1 und besitzt keine MAC Adresse. Daher ist er im Netzwerk unsichtbar und kann auch von keinem Angreifer erkannt werden
- Portabel, Modular oder virtuell, für Kupfer- und Glasfaser-basierte Netzwerke sowie virtuelle Umgebungen

Was für Vorteile bietet mir ein Netzwerk-TAP?

- 100%ige Sichtbarkeit/Transparenz garantiert
- Kein Packetverlust bei voll ausgelasteten Netzwerkverbindungen
- Unsichtbar im Netzwerk (kann nicht kompromitiert werden)
- Ausfallsicheres oder passives Design
- Spiegelt auch fehlerhafte CRC/FCS-Pakete
- Unterstützung von Vollduplex- und Microburst-Verkehrsanalysen
- Garantierte Datenintegrität
- Speziell gehärtete Modelle für IEC62443-Konformität

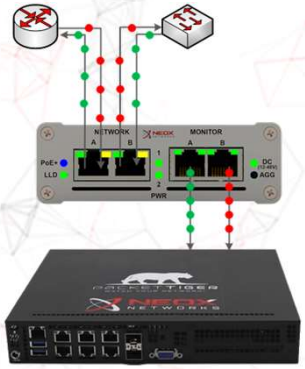
Die einzig zuverlässige Datenquelle!

Hohe Flexibilität durch verschiedene Betriebsarten



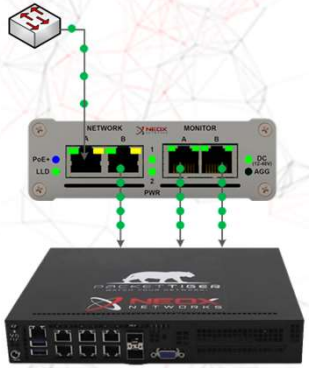
Aggregation Modus

- In diesem Modus werden die Datenströme **gebündelt** und **aggregiert** auf den beiden Monitoring Ports ausgegeben.
- Damit können Sie die Daten mehrerer Leitungen gleichzeitig mit einer einzigen Netzwerkschnittstelle an Ihrem Analysator auswerten.



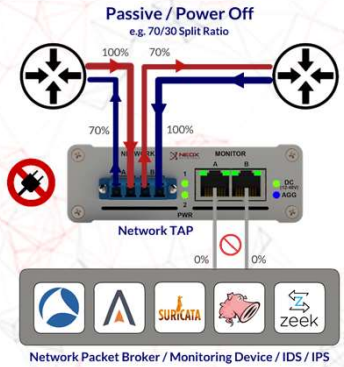
Breakout Modus

- Die Regeneration dient der Erfassung von **100 % Vollduplex-Verkehr**, der zur Analyse Ihres Netzwerks an mehrere Überwachungsgeräte (in diesem Fall bis zu 3) gesendet werden kann.
- In diesem Modus werden die Netzwerkgeschwindigkeitseinstellungen wie im Breakout-Modus synchronisiert.



Regeneration Modus

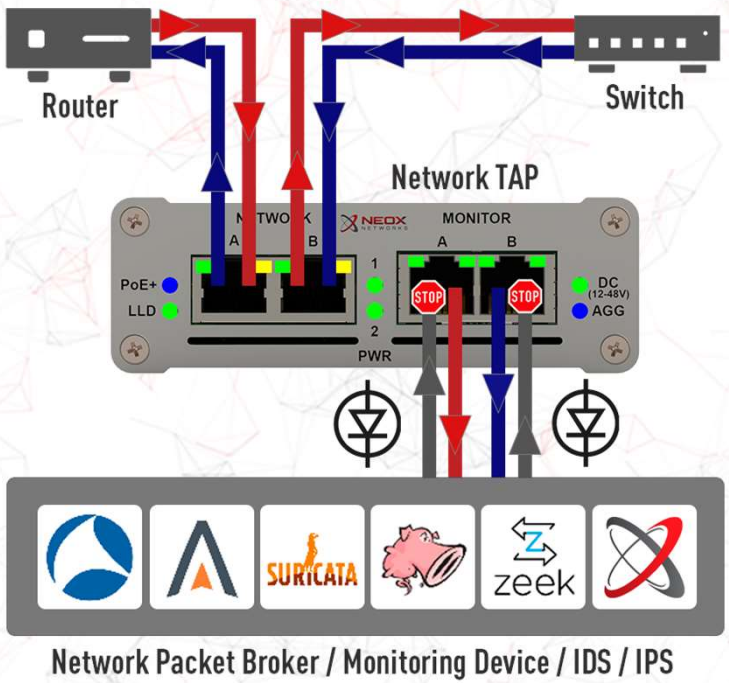
- Jede Richtung im TAP wird **separat gespiegelt.** Die Sende- und Empfangsrichtungen werden auf separaten Ports ausgegeben.
- In diesem Modus ist die eingestellte Netzwerkgeschwindigkeit für alle Ports gültig.



Passiv/Power-Off/Fail-Safe Modus

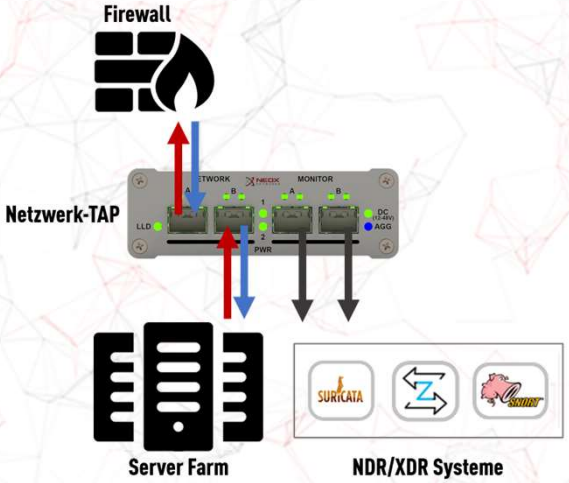
- Mittels Fail-Safe verhält sich der Kupfer-TAP im Falle eines Ausfalls oder einer willkürlichen Deaktivierung der Stromversorgung wie eine Kabelbrücke und sorgt dafür, dass die **aktive Netzwerkverbindung nicht unterbrochen** wird oder zumindest ohne die **TAP-Funktion weiter funktioniert**. Es kann zu einer Unterbrechung der Datenausleitung von einigen Millisekunden kommen.
- Beim passiven bzw. Power-Off Modus der hybriden und Fiber-TAPs hingegen kommt es auch bei einer Stromversorgungsunterbrechung zu keinem Paketverlust.

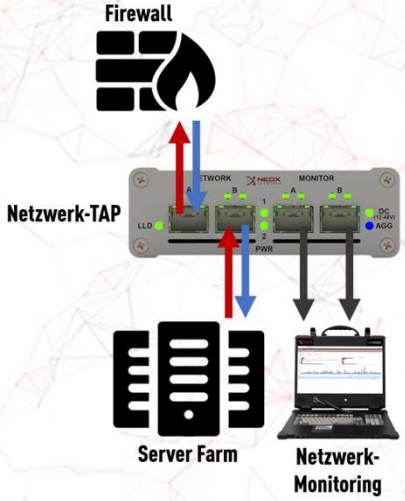
Wie funktioniert die Datendiode und was bringt sie mir?



- Datendioden gewährleisten eine unidirektionale Kommunikation und sorgen dafür, dass der ausgekoppelte Datenverkehr nur in eine Richtung fließen kann.
- Unidirektionale Netzwerkgeräte werden in der Regel eingesetzt, um Informationssicherheit zu gewährleisten oder kritische digitale Systeme wie industrielle Kontrollsysteme oder Produktionsnetze vor Cyberangriffen zu schützen.
- Durch das Hinzufügen dieser weiteren Sicherheitsebene wird eine Kompromittierung der Netzwerkverbindung und des Produktivnetzwerks verhindert.

TAPs in NDR/XDR- & Netzwerk-Monitoring Systemen

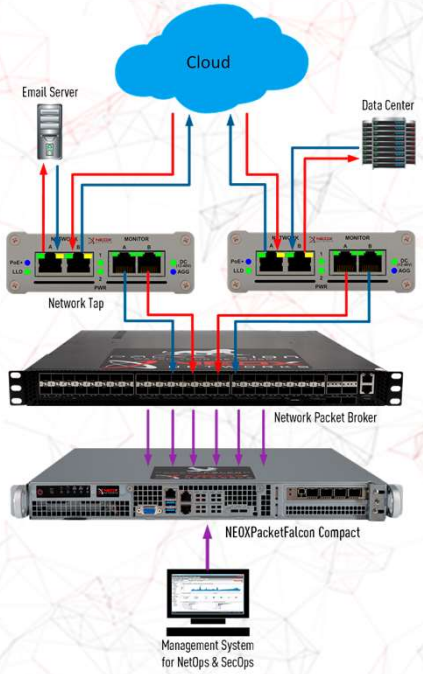




Jeder Netzwerk-TAP versorgt ein Tool mit Daten!

Deshalb benötigen Sie zuweilen einen Network Packet Broker, um wichtige Daten für ein oder mehrere Tools zu aggregieren oder zu filtern!

Tätern auf der Spur - TAPs in der Netzwerkforensik

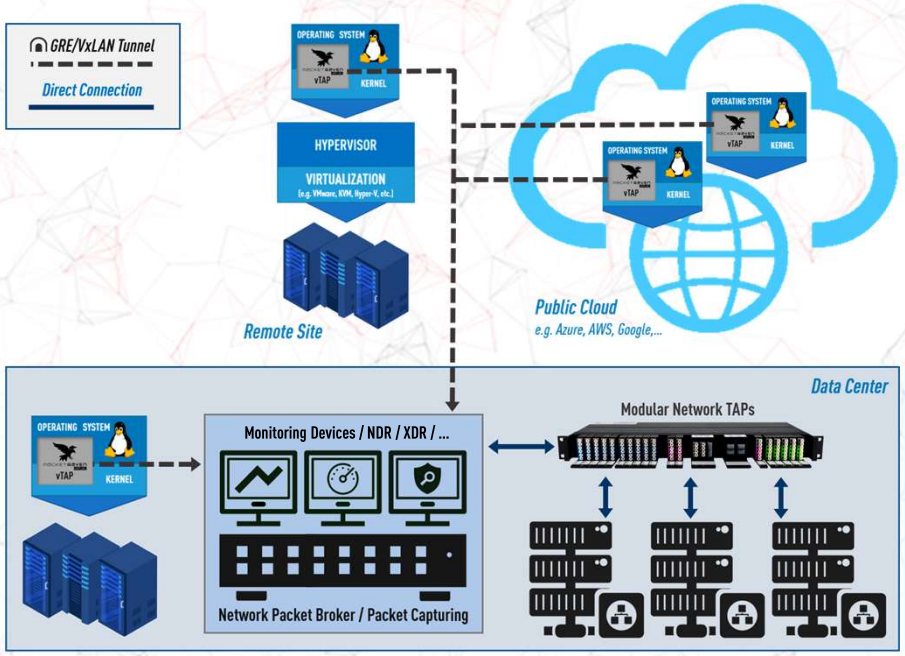


Die Netzwerkforensik ist ein Zweig der forensischen Wissenschaft, der die Sicherung von Beweisen in Computernetzen gewährleistet.

Dieser Bereich der forensischen Wissenschaft nutzt eine Vielzahl von Applikationen, wie z.B.:

- Analyse des gesamten Netzwerkverkehrs der beschuldigten Person in Gerichtsverfahren
- Rückverfolgung und Sicherung von Beweismitteln im Netz
- Analyse eines Systems nach einem Hack oder Cyberangriff

Cloud-Umgebungen überwachen mit Virtual TAPs



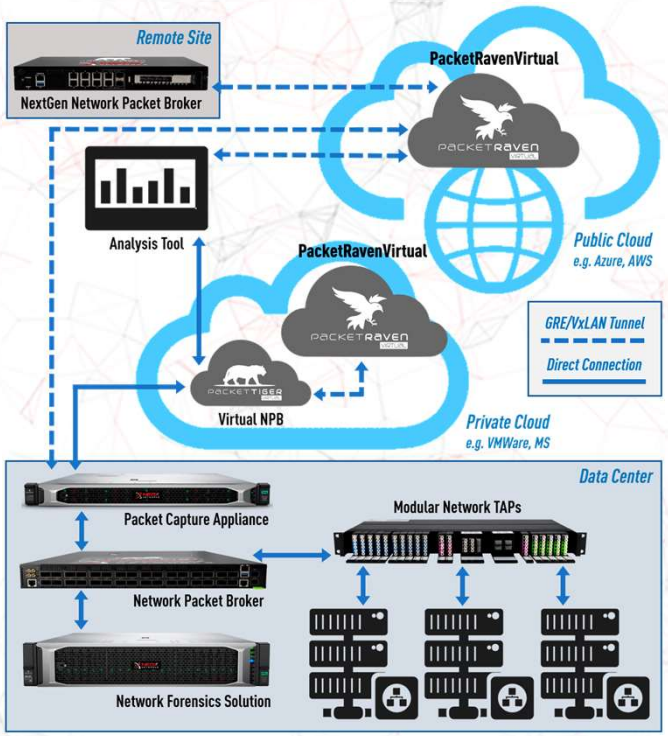
VORTEILE GEGENÜBER DEM VIRTUELLLEN PORT MIRRORING

- Granularere Zuordnung ist möglich, bspw. eine n:1 (Aggregation) oder eine 1:n (Regeneration).
- 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-Spiegelung nahezu unmöglich ist.
- Stateful Filtering, um nur relevante Daten zu kopieren und angeschlossene Tools zu entlasten
- Cloud-Anbieter behalten sich das Recht vor, etwaige Port-Spiegelung gemäß ihren Bedingungen einzuschränken.

ANWENDUNGSFÄLLE

- 100%ige Cloud-Transparenz für Sicherheit, Analyse und Fehlerbehebung
- Verstärkung der Sicherheitsabwehr
- Verringerung von Performance-Problemen
- Konsolidierung von Initiativen zur Einhaltung von Compliance Regularien

Monitoring über alle Perimeter hinweg



Um 100% Netzwerktransparenz zu erhalten ist ein Zusammenspiel mehrerer Netzwerkkomponenten notwendig.

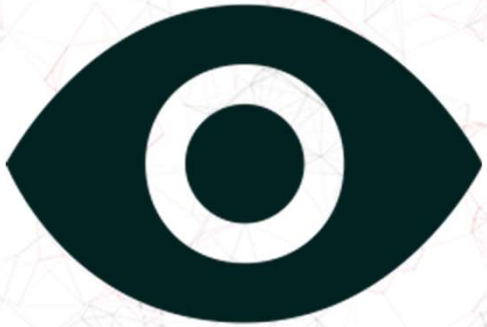
Netzwerk-TAPs bilden dafür die

Grundvoraussetzung!

HABEN AUCH SIE TOTE WINKEL IN IHREM NETZWERK?

TRANSPARENZ

Das Fundament für Ihre Netzwerksicherheit



RUFEN SIE UNS AN

T: +49 6103 37 215-910

SCHREIBEN SIE UNS EINE EMAIL

solutions@neox-networks.com

CHATTEN SIE MIT UNS

www.neox-networks.com