NETZWERKE FÜR DAS 3. JAHRTAUSEND

IP ADDRESS MANAGEMENT

PRIVILEGE MANAGEMENT

AD & CLOUD AUDITING

n3k NETWORK SYSTEMS

runIP Radar

Sicherheit & Kontrolle für Ihre DNS- und DHCP-Infrastruktur

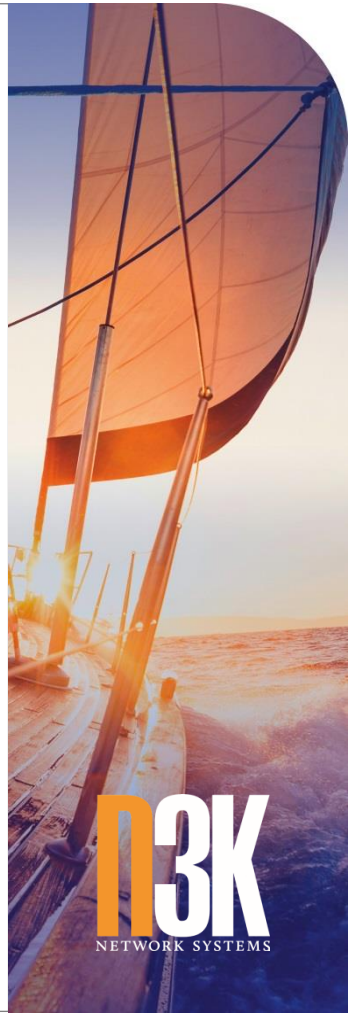
n3k NETWORK SYSTEMS

Die Bedeutung von DNS für die Netzwerksicherheit

n3k NETWORK SYSTEMS

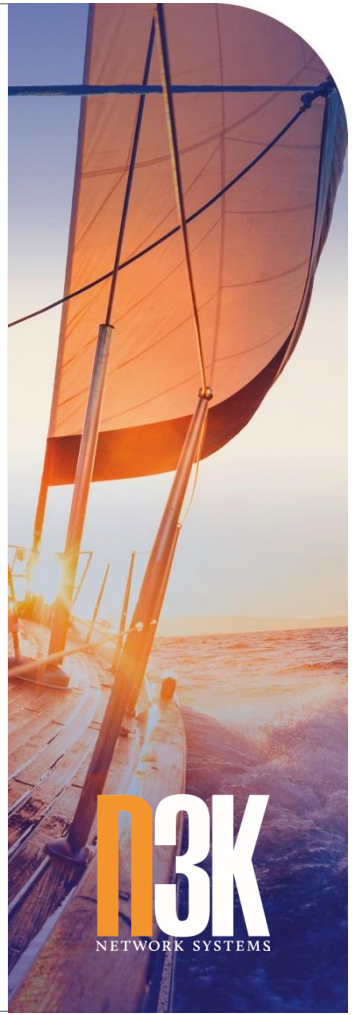
Die Bedeutung von DNS-Sicherheit

- Das Domain Name System DNS ist der kritischste Netzwerkdienst in TCP/IP-Netzwerken
  - Ohne DNS ist für die Mehrzahl der internen und externen Applikationen keine Konnektivität gewährleistet
  - *„When DNS is down the network is down“*
- DNS spielt auch in Angriffsszenarien eine bedeutende Rolle
  - DNS ist in aller Regel auf Firewalls freigeschaltet
    - DNS-Tunnel zur Umgehung von Zugriffsregeln von Gast-WLAN
    - Kommunikationskanal für Command & Control für Malware
    - Exfiltration von Daten über DNS-Tunnel
      - Tools hierfür frei erhältlich, z.B. „AndIodine“ als Smartphone-App



Die Bedeutung von DNS-Sicherheit

- DNS selbst ist häufiges Ziel von Angriffen
  - DDoS-Angriffe auf DNS, z.B. DNS Amplification Attacks
  - Ausnutzung von Schwachstellen auf DNS-Servern, z.B. Cache Poisoning
- Gelingt es einem Angreifer, die Kontrolle über DNS-Server oder auch nur einzelne DNS-Einträge zu erhalten, kann er die Benutzer böswillig auf eigene Server umleiten
  - Webseitenverunstaltung gehört dann noch zu den harmloseren Folgen
- DNS-Protokolle liefern wertvolle Informationen
  - Bei der forensischen Analyse von möglichen Angriffen, kann es von großem Nutzen sein, rückwirkend die DNS-Abfragen einzelner Clients nachvollziehen zu können

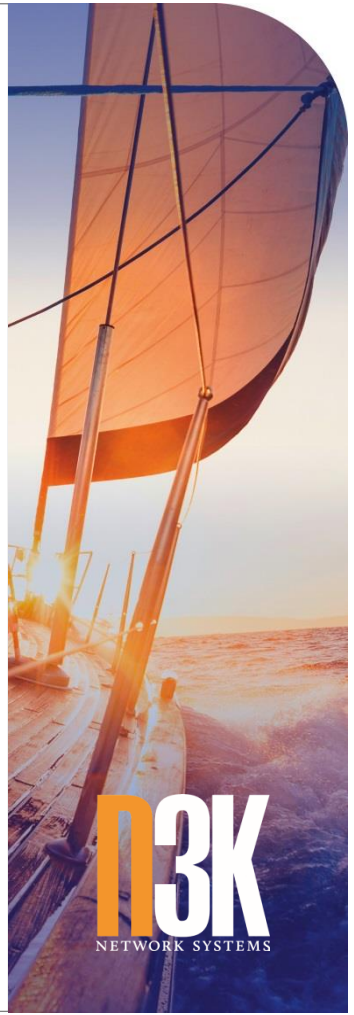


Die Antwort:
runIP Radar

n3k
NETWORK SYSTEMS

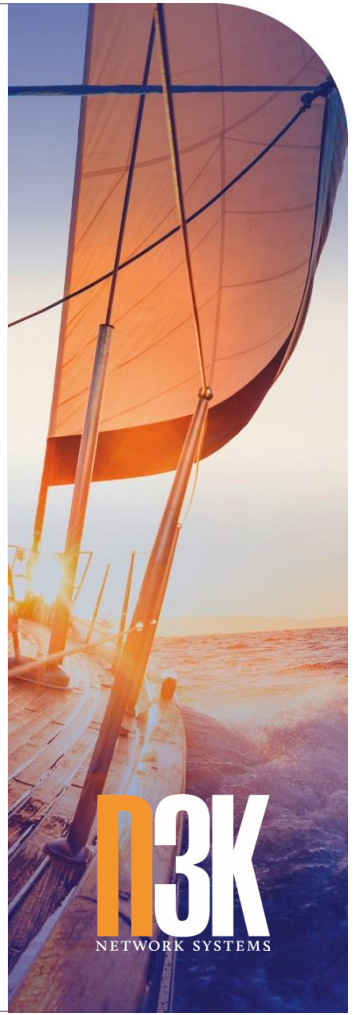
Die Antwort: runIP Radar

- runIP Radar
  - liest den kompletten DNS-Verkehr mit
  - erkennt DNS-Tunnel und kann sie blockieren
  - erkennt weitere DNS-Anomalien
    - z.B. den sprunghaften Anstieg von DNS-Anfragen auf einem Client
  - protokolliert sämtliche DNS-Anfragen
  - protokolliert sämtliche DNS-Antworten
  - lässt sich mit RPZ-Feeds integrieren
    - So können bekannte Malware-Ziele von vorneherein geblockt werden
- runIP Radar verbessert damit signifikant die Sicherheit Ihrer DNS-Infrastruktur



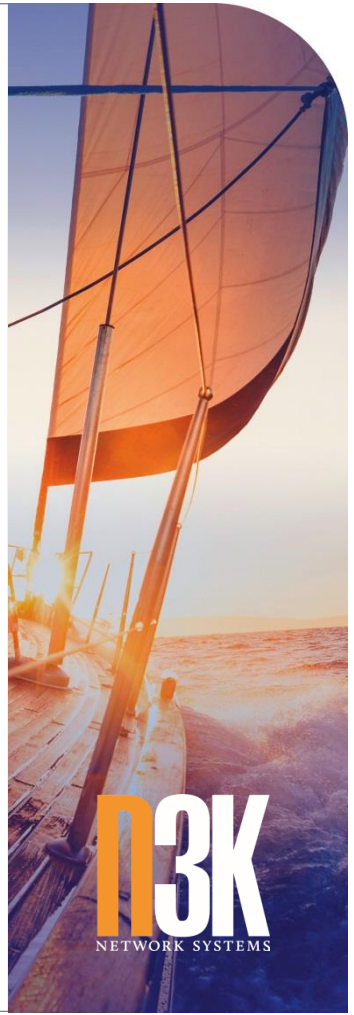
runIP Radar – Aufbau und Grundfunktion

- runIP Radar ist als Add-On für runIP implementiert
  - Läuft als Dienst auf den einzelnen runIP DNS/DHCP-Appliances
- Dezentrale Erkennung von DNS-Anomalien, insbesondere von DNS-Tunneling
  - Alarmierung und ggf. Sperrung bei auffälligem Verhalten
- Optimiertes Logging von DNS-Queries und -Responses sowie von DHCP-Messages
  - Performanter, umfassender und flexibler als mit BIND-Mitteln
  - Weiterleitungsmöglichkeit an SIEM-Lösungen wie Splunk/ArcSight
- Einbindung von externem RPZ-Feed über Partner



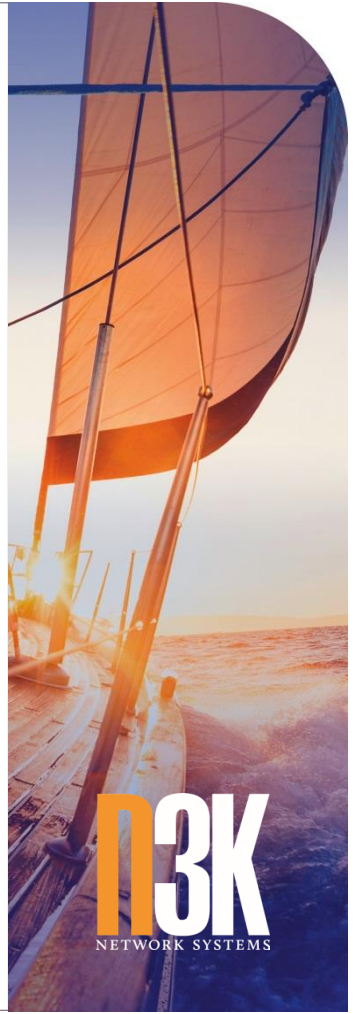
Details zu Version 1.0

- Erkennung von DNS-Anomalien
  - Schnelle Erkennung bekannter DNS-Tunneling-Tools
  - Konfiguration, ob alarmiert wird und ob gesperrt wird
  - Definition von Domain-Whitelists
- Sperrung von Problem-Clients und Problem-Zielen
  - Die Sperrung erfolgt technisch mit Hilfe von RPZ-Zonen
  - Während die Erkennung dezentral stattfindet, werden die erzeugten RPZ-Regeln an die weiteren DNS-Server weiterverteilt
- Benutzerdefinierte Thresholds für die Query-Anzahl auf Basis von IP-Adressen oder IP-Adressbereichen
  - Sicherstellen, dasd Systeme wie z.B. Mail-Server oder HTTP-Proxy-Server nicht gesperrt werden



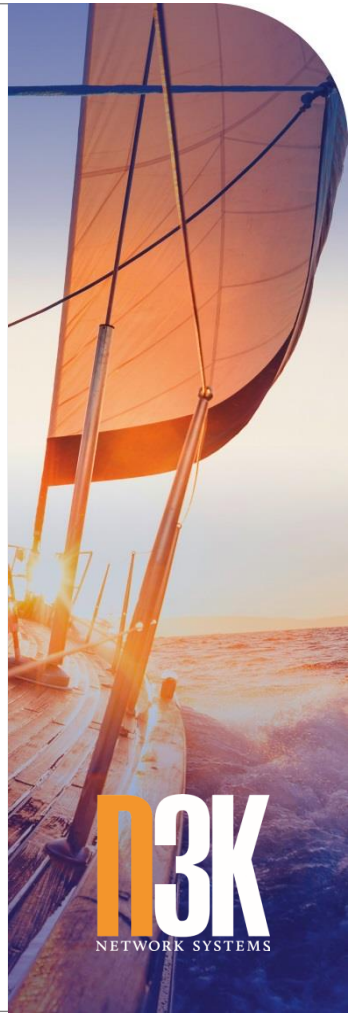
Details zu Version 1.0

- Wenig invasiver Ansatz
  - Queries und Responses werden nur mitgelesen, Sperrung ausschließlich durch BIND-RPZ-Mechanismus
  - Performance-optimierte Implementierung
- Optimiertes Logging von DNS-Queries sowie von DNS-Responses
  - Performanter, umfassender und flexibler als mit Bind-Mitteln
  - Weiterleitungsmöglichkeit an SIEM-Lösungen wie Splunk oder ArcSight
    - Zunächst per Rsyslog, später ggf. optimierte Schnittstellen
  - Definition von Domain-Listen, die vom Logging und/oder der Weiterleitung ausgenommen sind, z.B. Beschränkung auf externe Domain-Namen
  - Definition der technischen Attribute, die geloggt werden sollen



Details zu Version 1.0

- Einbindung von externem RPZ-Feed
  - N3K bietet Feeds von mehreren geeigneten Partnern an
  - Kunde kann alternativ oder zusätzlich andere RPZ-Feeds einbinden
- runIP-Integration
  - Verteilung der Konfiguration über runIP-Konfig-Paket
  - Möglichkeit, Alarme zentral auf der runIP Management Station zu sammeln und von dort zentral weiterzuleiten
    - Es werden im runIP-Monitoring sowohl runIP-Radar-Alarme protokolliert als auch RPZ-Treffer (runIP-Radar-RPZ-Zone und andere RPZ-Zonen)
  - Monitoring des Dienstes
- runIP Radar 1.0 ist seit Februar 2019 verfügbar

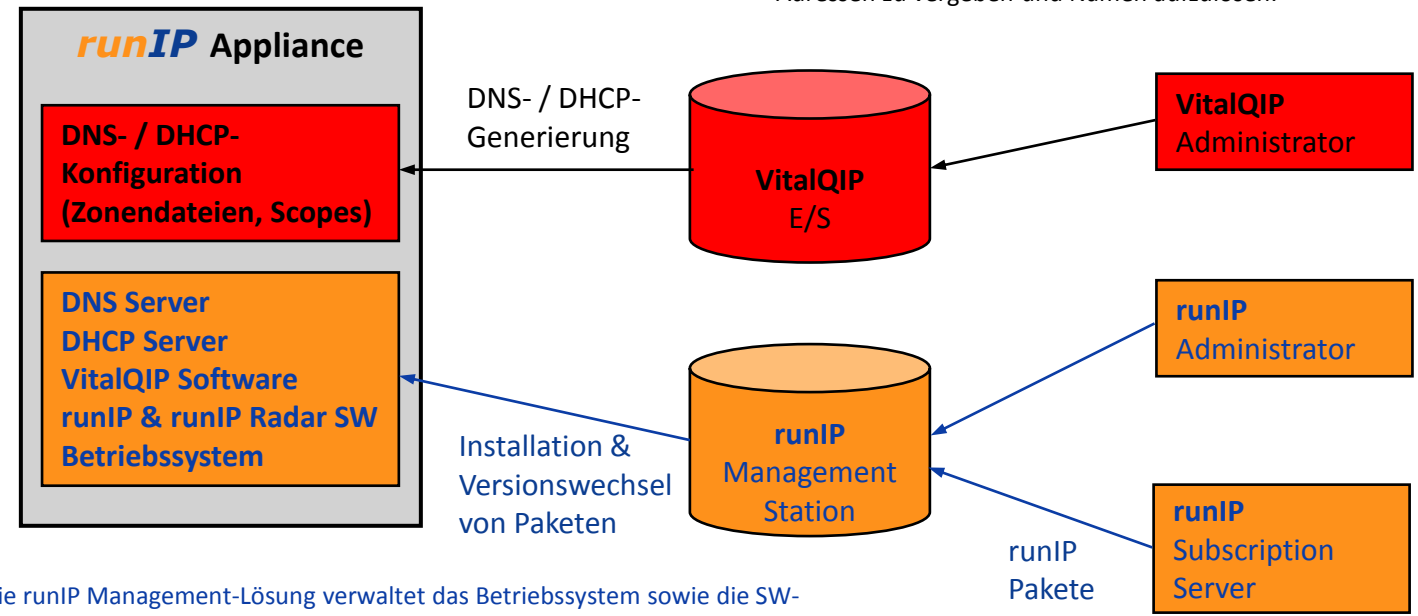


Architektur

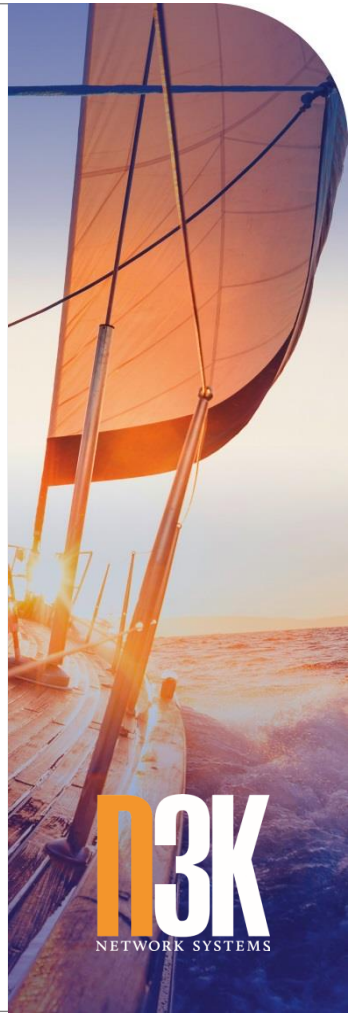
n3k NETWORK SYSTEMS

ZUSAMMENSPIEL RUNIP MIT VITALQIP

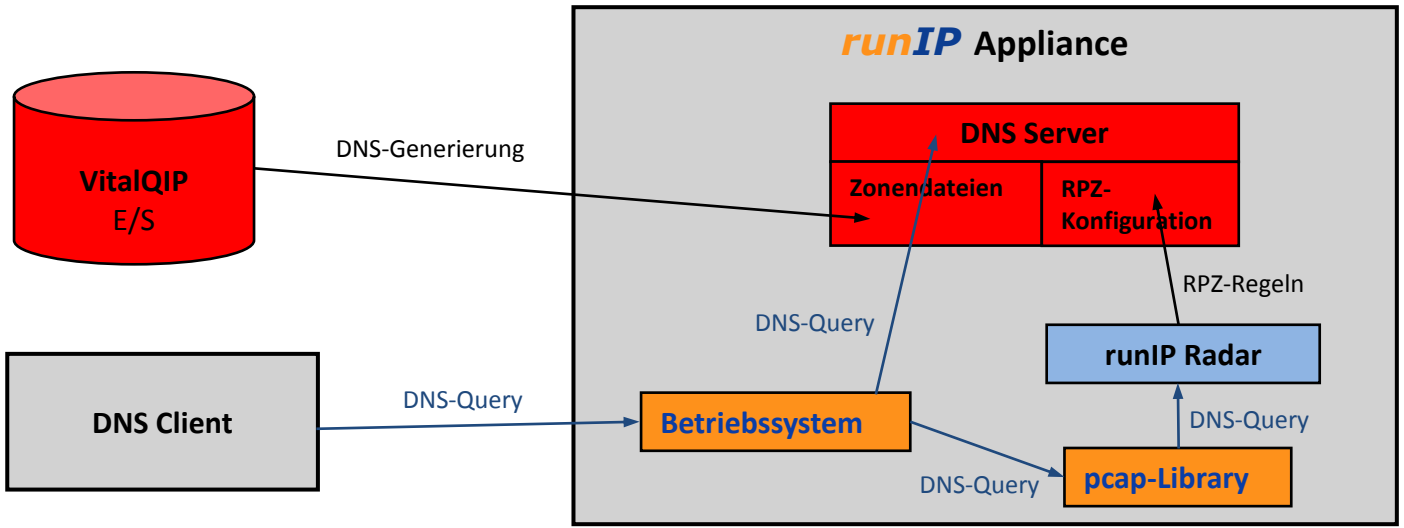
Die VitalQIP-Umgebung verwaltet die Daten, die von den DNS- und DHCP-Servern auf den Appliances benötigt werden, um Adressen zu vergeben und Namen aufzulösen.



Die runIP Management-Lösung verwaltet das Betriebssystem sowie die SW-Versionen der DNS- und DHCP-Server, die auf der Appliance aktiv sind. Der runIP Administrator lädt runIP-Pakete vom runIP Subscription Server herunter und aktiviert sie nach Bedarf auf den runIP Appliances.
Zusätzlich verteilt runIP die SW und Konfiguration für runIP selbst und runIP Radar.

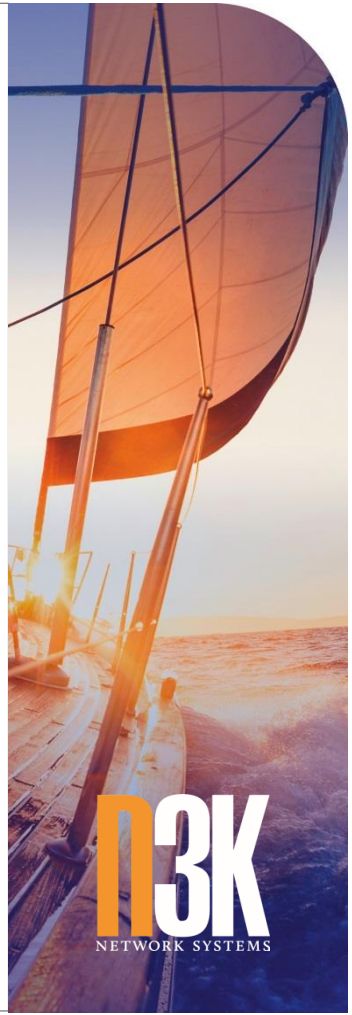


Zusammenspiel runIP Radar, VitalQIP und DNS-Server (BIND) – DNS Queries

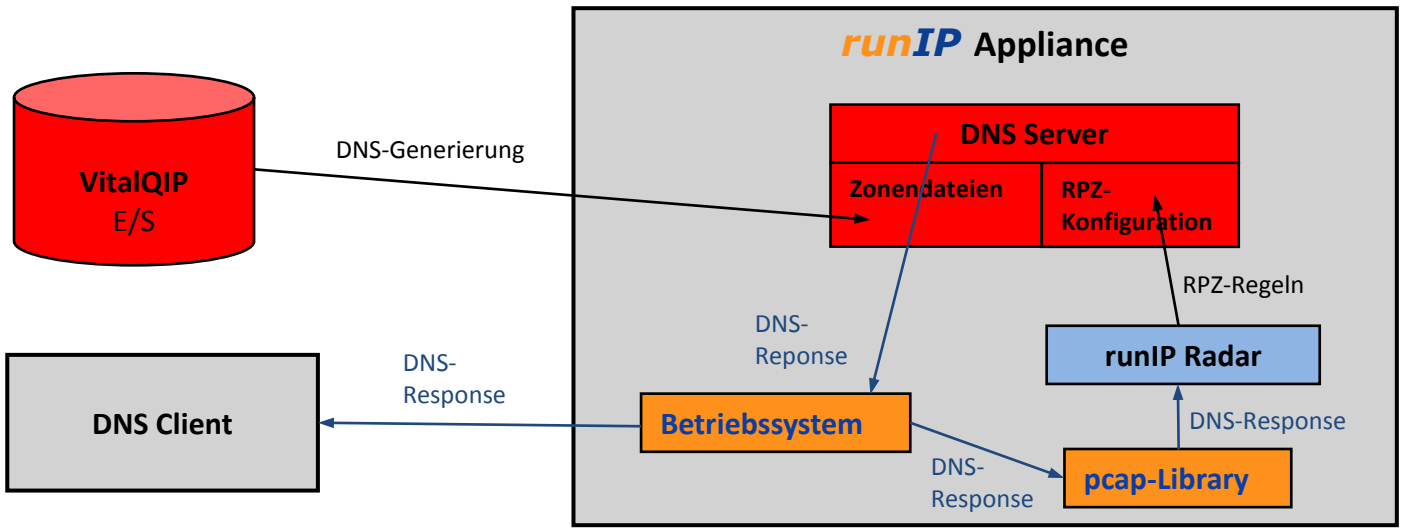


runIP Radar liest sämtlichen DNS-Verkehr (Queries & Responses) mit Hilfe der pcap-Library mit. Aufgrund der Regelbasis werden Alarme erzeugt und ggf. RPZ-Regeln zwecks Alarmierung / Sperrung per dynamischen DNS-Updates an den DNS-Server geschickt.

Query-Verarbeitung:
Die vom DNS-Client an die Appliance geschickten DNS-Queries werden an den DNS-Server sowie über die pcap-Library an runIP Radar weitergeleitet.

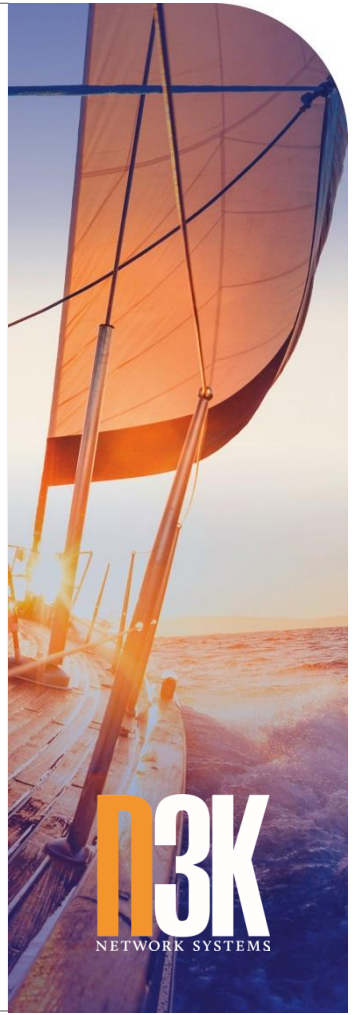


Zusammenspiel runIP Radar, VitalQIP und DNS-Server (BIND) – DNS Responses



runIP Radar liest sämtlichen DNS-Verkehr (Queries & Responses) mit Hilfe der pcap-Library mit. Aufgrund der Regelbasis werden Alarme erzeugt und ggf. RPZ-Regeln zwecks Alarmierung / Sperrung per dynamischen DNS-Updates an den DNS-Server geschickt.

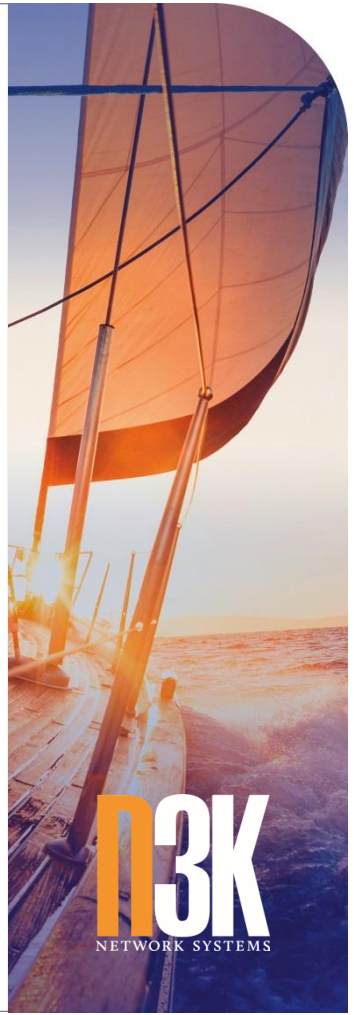
Response-Verarbeitung:
Die vom DNS-Server erzeugten DNS-Responses werden an den anfragenden DNS-Client geschickt sowie über die pcap-Library an runIP Radar weitergeleitet.



Roadmap

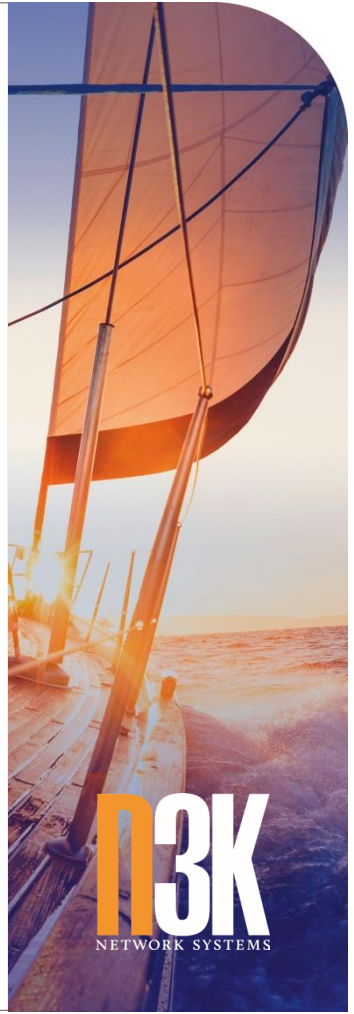
Ausblick – Version 1.1

- Protokollierung des DHCP-Traffics
  - Umfangreiches Logging der DHCP-Transaktionen
  - Definition der technischen Attribute, die geloggt werden sollen
  - Weiterleitungsmöglichkeit an SIEM-Lösungen wie Splunk oder ArcSight
  - Definition von Ausnahme-Listen, z.B. für DHCP-Probes
- In Kürze verfügbar



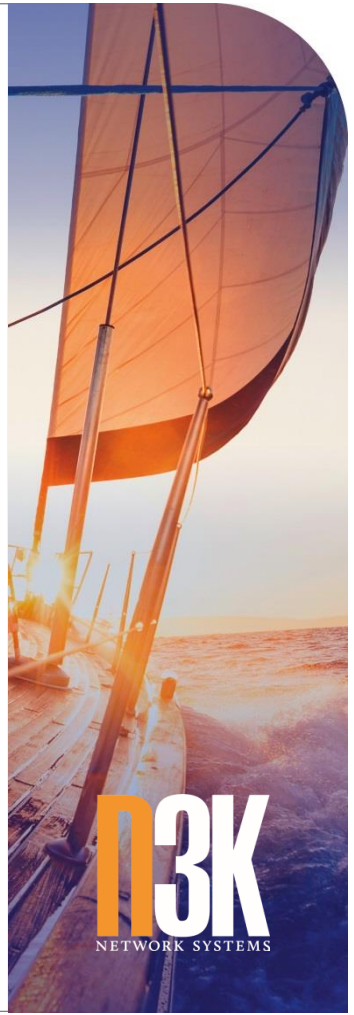
Ausblick – Version 2.0 (Teil 1)

- GUI-basierte Steuerung und Auswertung
  - Komfortablere und übersichtlichere Steuerung
  - Auditing von Änderungen
  - Umfangreiches GUI-basiertes Reporting
    - Tabellendarstellung mit Filter-Such-Möglichkeiten für
      - Rate-Limit-Überschreitungen
      - Erkannte Anomalien
      - Eigene und fremde RPZ-Treffer
    - Möglichkeit, übers GUI gezielt in DNS- und DHCP-Verkehrsdaten zu suchen
      - Dezentral und zentral
    - Vorgefertigte Reports wie Top-Clients, Top-Domains, Top-FQDNs
    - runIP-Statistics für Alarmierungen / RPZ-Treffer



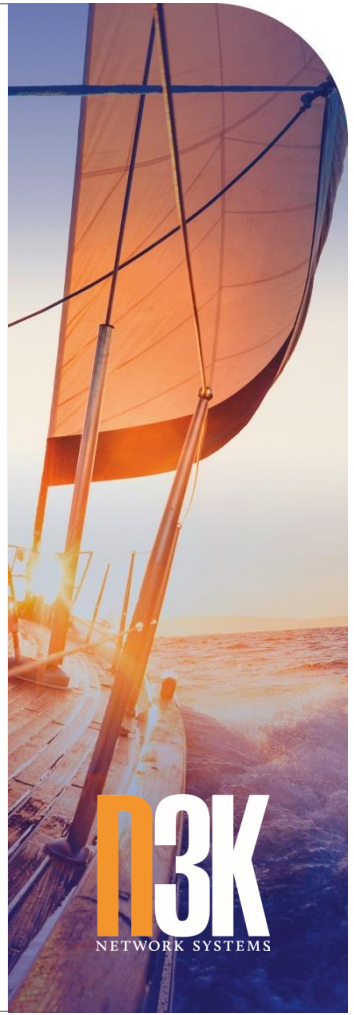
Ausblick – Version 2.0 (Teil 2)

- GUI-basierte Steuerung und Auswertung
  - Möglichkeit, gesperrte Clients / Domains manuell wieder zu entsperren
  - Troubleshooting über komfortables Live-Logging mit Filter- und Suchmöglichkeiten übers GUI
- Geplant für Mitte 2020



Ausblick – Version 3.0

- Version 3.0
  - Langzeit-Archivierung mit entsprechenden Auswertungsmöglichkeiten
  - Evtl. Technische Umsetzung unabhängig von runIP
- Änderungen vorbehalten



NETZWERKE FÜR DAS 3. JAHRTAUSEND

n3k NETWORK SYSTEMS