Factsheet

RUNIP RADAR

runIP | RADAR

Security and Visibility for your DNS-and DHCP-Environment

In modern TCP/IP networks, DNS is one of the most critical network services, as name resolution plays a central role in the connectivity of systems and applications. DNS is therefore also one of the preferred targets of malicious actors on the internet. This is mainly because by controlling a DNS server, users can be specifically redirected to servers of the attacker. In addition, DNS is also used for DDoS attacks, primarily via DNS amplification. In this case, an attacker sends small DNS queries with the spoofed address of his victim to a DNS server with the aim of generating the largest possible responses, which the DNS server then sends to the victim. In this way, the attacker can amplify his attack by a factor of up to 50 (hence amplification). Finally, DNS plays a role in many other attack scenarios, for example as a communication channel for command & control servers or in the exfiltration of data via DNS tunnels - i.e. a mostly inconspicuous data theft.

Securing DNS is especially important because a compromise of this service can significantly impact the availability of almost all applications. While DDI solutions simplify the operation of DNS and DHCP, they usually do not include targeted security measures to ensure the availability of the services at all times. runIP RADAR closes this gap and enables an efficient and robust protection of the DNS infrastructure.

Features in detail - alerting and blocking

runIP RADAR allows the definition of rate limits, which can be used to specifically block clients and/or targets when exceeded. If required, this blocking can also include the client and the domain used. For individual address ranges or domains, automatic unblocking after defined times can also be configured. In this way, it is possible to ensure, for example, that the address ranges of guest WLANs are not permanently blocked after a security incident. Even blockings that occurred due to ongoing attacks against the domain can be lifted after a certain security period without manual intervention.

Features in detail - Logging

runIP RADAR is capable of logging all DNS and DHCP traffic in the network in a decentralized manner or forwarding it centrally to an existing system at the customer‘s site. The technical attributes to be logged are freely configurable. In addition, exception lists can be defined, for example for trusted networks or DHCP probes. The ability to forward log data to SIEM systems allows easy integration into enterprise-wide security solutions and correlation of the logged data with security events generated by other security solutions. For example, attacks on the DNS infrastructure can be quickly and reliably detected and mitigated or blocked.

Your benefit

- Full protection of your DNS infrastructure
- Fast detection of DNS tunnels
- Extensive prevention of data exfiltration via DNS
- Defense against DDoS attacks against the DNS infrastructure
- Support for forensic analysis after security incidents
- Tight integration with the runIP management platform

Integration into the runIP services platform

runIP RADAR runs as a service on N3K‘s runIP appliances. It is managed and configured via a separate web interface. The RADAR server handles the entire configuration of runIP RADAR, which is replicated to all runIP appliances within the network.

runIP | RADAR

GUI-based reporting

The RADAR server has an intuitive GUI, which is used to configure and control the RADAR server and all instances of runIP RADAR on the individual runIP appliances. The GUI offers a large number of predefined reports as well as easy options to create individual reports. In addition, the GUI provides easy-to-understand statistics on alerts and RPN hits. Pre-built reports include:

- Rate limit overruns indicating unwanted data exchange.
- Use of already blocked DNS domains and client IPs
- Top clients, top domains or top FQDNs including frequently used names that cannot be resolved.

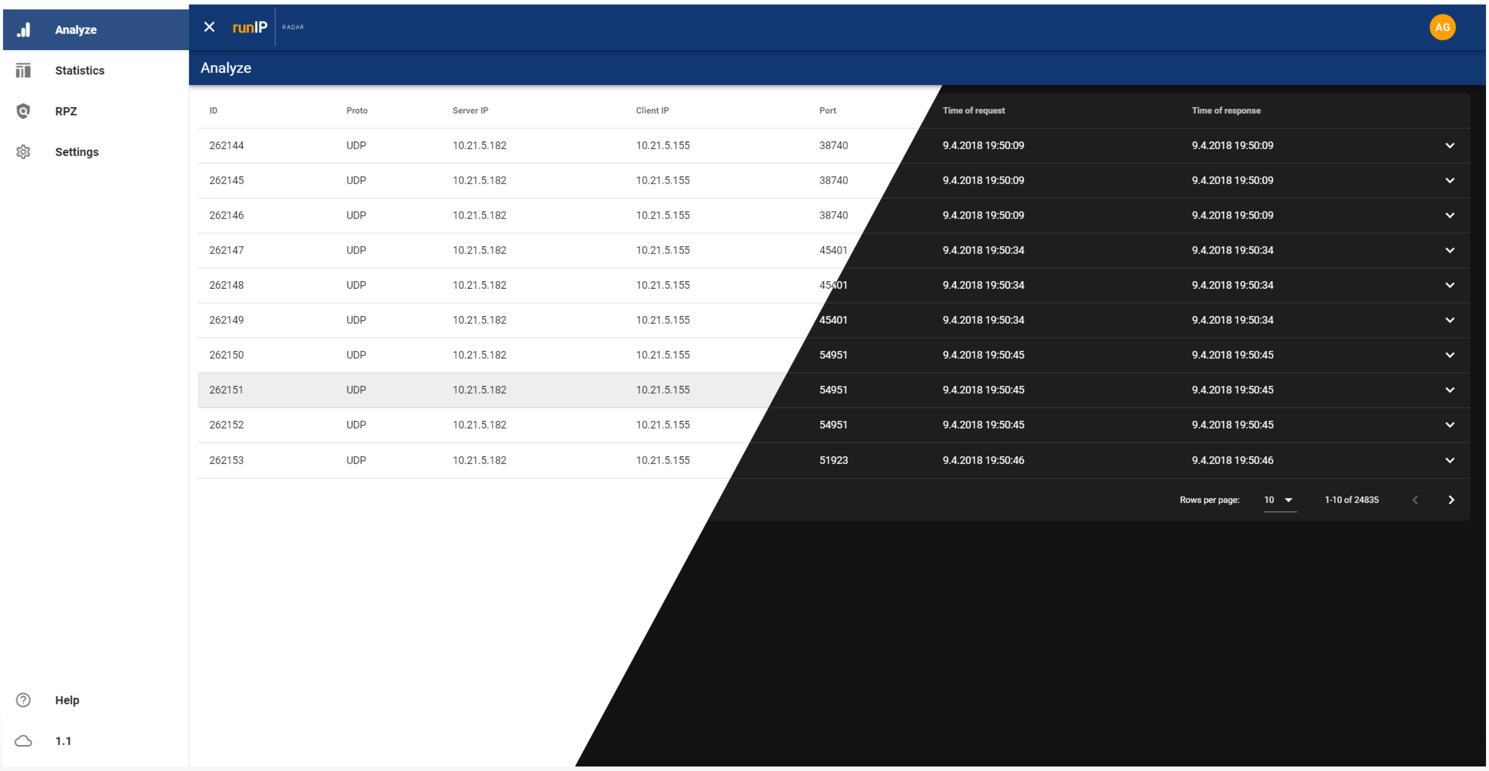
Independent of the DDI solution

runIP RADAR is based on N3K's extensive DDI expertise and can currently be used with all DDI solutions supported by the runIP DDI PLATFORM:

- Nokia VitalQIP
- BT Diamond IPControl
- Men & Mice Micetro

runIP RADAR benefits from the (optional) high availability of the runIP hardware, so that DNS security can be guaranteed at any time.

In a later version, runIP RADAR will be completely independent of runIP and thus support all DDI solutions on the market.



Analyze

ID	Proto	Server IP	Client IP	Port	Time of request	Time of response
262144	UDP	10.21.5.182	10.21.5.155	38740	9.4.2018 19:50:09	9.4.2018 19:50:09
262145	UDP	10.21.5.182	10.21.5.155	38740	9.4.2018 19:50:09	9.4.2018 19:50:09
262146	UDP	10.21.5.182	10.21.5.155	38740	9.4.2018 19:50:09	9.4.2018 19:50:09
262147	UDP	10.21.5.182	10.21.5.155	45401	9.4.2018 19:50:34	9.4.2018 19:50:34
262148	UDP	10.21.5.182	10.21.5.155	45401	9.4.2018 19:50:34	9.4.2018 19:50:34
262149	UDP	10.21.5.182	10.21.5.155	45401	9.4.2018 19:50:34	9.4.2018 19:50:34
262150	UDP	10.21.5.182	10.21.5.155	54951	9.4.2018 19:50:45	9.4.2018 19:50:45
262151	UDP	10.21.5.182	10.21.5.155	54951	9.4.2018 19:50:45	9.4.2018 19:50:45
262152	UDP	10.21.5.182	10.21.5.155	54951	9.4.2018 19:50:45	9.4.2018 19:50:45
262153	UDP	10.21.5.182	10.21.5.155	51923	9.4.2018 19:50:46	9.4.2018 19:50:46

Rows per page: 10 1-10 of 24835

About N3K: Fast growing IP networks require comprehensive professional solutions for key aspects of network management. N3K specializes in solutions for DNS, DHCP & IP Address Management (DDI), Active Directory& Cloud Auditing, and Privilege Management. Strong focus has developed a very high level of expertise and experience. This has resulted in a history of successful and effective project delivery to fully meet the individualrequirements of a high quality, diverse customer base. As a result, N3K has become a very successful business. N3K supports customers throughout the entire project cycle - analysis, design, project planning, implementationand training. After implementation, the company delivers extensive ongoing maintenance and support services including global 7x24 support. The company tag line „Networks for the third millennium" expresses a deep belief in the long term. Over the life of the company this is demonstrated by a history of successful cooperation with both suppliers and a broad range of customers drawn from a wide selection of vertical industries. Based on this philosophy, N3K Network Systems has established itself as a leading provider in Germany - more than half of the DAX companies now rely on n3k products and services. With locations in the US and Singapore, services can be provided worldwide.

n3K NETWORK SYSTEMS