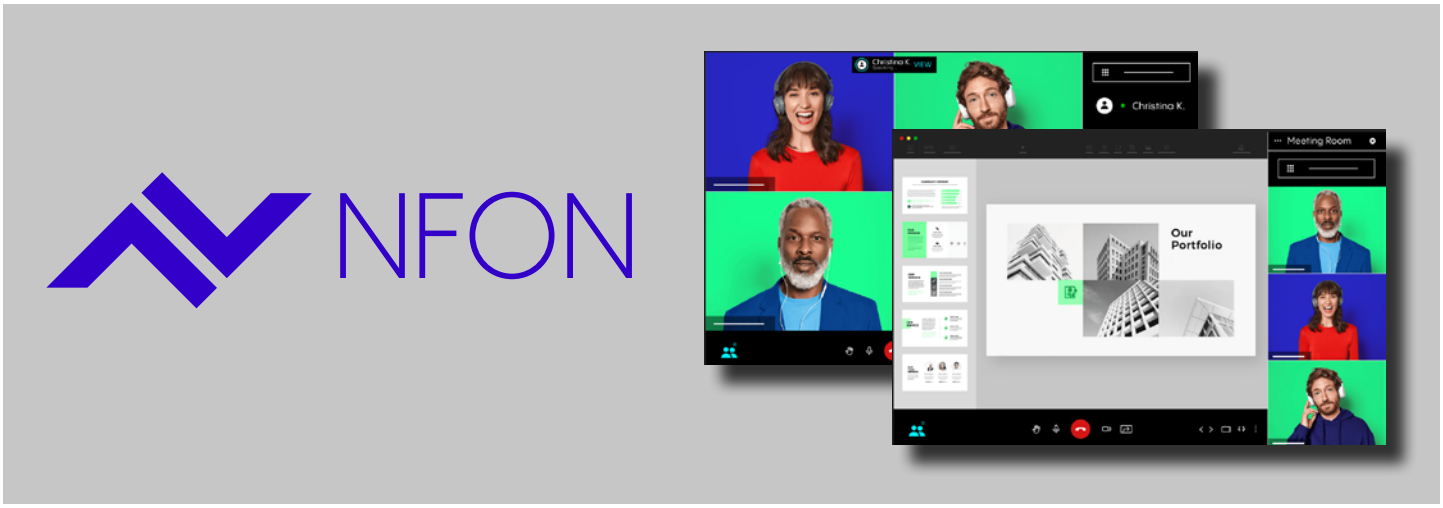
MYRA

CASE STUDY

Securing Cloud Communications Services Requires a Custom Approach

Case Study
NFON

Solutions
DDoS Protection
Hyperscale WAF
Secure DNS



Essential & Highly Complex: How NFON Protects IP Telephony from Cyber Criminals

Executive Summary

With more than 50,000 customers, NFON AG is the leading European provider of cloud-based telephone systems. The company is active in 15 European countries and has more than 500 employees. Digital communication solutions have become an integral part of everyday life for most companies. Especially since the start of the coronavirus pandemic, unified communication solutions from the cloud have become the tool of choice for many companies to connect customers, partners, and employees – regardless of location. The protection of such essential digital services is crucial to safeguard the operational business of these companies against outages. This is why NFON has been protecting its VoIP services with security-as-a-service solutions from Myra Security since 2014.

Objective

Protecting VoIP technologies against DDoS attacks is extremely complex, as IP telephony generates large volumes of connectionless UDP traffic. This data traffic is difficult or impossible to qualify using conventional protection methods. In the event of an attack, malicious traffic can therefore not be distinguished from regular requests, which prevents successful mitigation of the attack. A suitable solution had to be found for this technological hurdle.

Technically, VoIP protection is provided via DDoS protection for infrastructures and data centers (layer 3/4). In addition to the implemented DDoS protection, NFON relies on the Myra Hyperscale WAF (Web Application Firewall) on Layer 7, to protect legacy applications, for example, from cyberattacks. Myra Secure DNS is also used to protect the name resolution of NFON domains.

Dynamic Allowlisting

To overcome the challenge of traffic qualification, Myra developed a dynamic allowlisting solution together with NFON. NFON periodically records the IPs of registered and authenticated end devices and other authenticated connections and stores them in an IP set for allowlisting at Myra. In the event of an actual attack, only the signaling protocols and the audio/video packets of the already registered clients are initially allowed through. The challenge of this solution lies in the fact that tens of thousands of IP addresses have to be reliably recorded and managed every hour.

Implementation by Infrastructure Protection

Myra's protection technologies are entirely independent of the existing infrastructure and can be implemented quickly because they do not require any additional hardware or software. Myra takes care of almost the entire setup and configuration of the services. The effort on the customer side is minimal.

To connect the infrastructure protection, the customer first creates the RIPE route objects for their networks in accordance with Myra's specifications. The Myra Network Operations Center (NOC) team of experts takes care of the configuration for the networks. In the event of an attack, Myra uses "More Specific" announcements to pull all incoming traffic to its own scrubbing centers. There, the attack traffic is discarded and the remaining clean traffic is forwarded back to the customer via a previously agreed connection. To automate this switchover, Myra can evaluate the customer's flow data. The customer provides a virtual machine for this purpose, the Myra experts define the threshold values and regularly compare them with the customer. Direct connections, virtual LAN connections, GRE tunnels and IPSec are available for traffic forwarding. In the case of NFON, clean traffic is transferred between Myra and the customer infrastructure via two GRE tunnels.

Secure DNS and Hyperscale WAF

The migration of name resolution, including the associated configuration, from NFON to Myra Secure DNS can be delegated with little effort thanks to Hidden Primary. The Myra DNS servers use anycast for routing, which ensures optimum performance with high redundancy.

The technical implementation of Layer 7 for the WAF protection system is basically possible in two ways: Either the DNS entry is adapted via the CNAME entry or the authoritative DNS server is transferred to Myra using an import of existing zones. As soon as the customer's corresponding TLS certificates have been made available in the Myra dashboard via API or upload, the TLS connection can be terminated and a deep packet inspection carried out. The Myra NOC then configures the filter rules in close coordination with the customer. Customized filters allow granular traffic control to intercept malicious or suspicious requests with the Myra Hyperscale WAF even before they reach the systems of NFON and its customers.

Data Protection & Compliance "Made in Germany"

Confidentiality and integrity are at least as important in electronic communication via VoIP as technical security. In light of this, it was crucial for NFON to choose a German company that met the same strict data protection and security requirements as NFON. With a highly certified provider such as Myra (BSI ISO 27001 based on IT-Grundschutz, PCI-DSS certified, IDW PS 951 type 2 (ISAE 3402) tested, KRITIS qualified, BSI C5, Trusted Cloud) NFON achieves more legal compliance and GDPR compliance.

These characteristics also help to attract strategic business partners such as Deutsche Telekom, which secures its IT projects through sophisticated PSA (Privacy and Security Assessment) procedures. For a successful cooperation, security and data protection at the highest level are required - both at NFON itself and with affiliated service providers.

Summary

Since the launch of Myra protection services, NFON has benefited from tailored security solutions that meet the special requirements of modern cloud communication in the corporate environment. The company's IP telephony solutions are thus reliably protected against cyberattacks - and this in full compliance with the strictest data protection requirements.

Jan-Peter Koopmann, Board member and CTO at NFON, sums up the successful collaboration with Myra as follows: "Myra has developed a product for us that provides essential protection for NFON's IP telephony services. No other provider could supply us with a comparable solution in this tailor-made form. At Myra, we receive individual services that also meet our high standards of privacy and compliance."

Working with Myra Offers NFON the Following Benefits:

- DDoS protection with dynamic allowlisting for VoIP services
- Protecting legacy applications with Hyperscale WAF
- Securing name resolution with Myra Secure DNS
- Legally compliant partnership with a highly certified provider from Germany
- Made in Germany, legally compliant with GDPR
- Local 24/7 support from Germany via the Myra NOC at the headquarters in Munich

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0667-2024 | PCI DSS Certified | BSIG KRITIS-qualifiziert | BSI C5 TESTAT TYP 2 | Trusted Cloud SERVICE 10043 | ISAE 3402 IDW PS 951 TYPE 2 | KRITIS Nachweis gemäß § 8a. Abs. 3 BSIG

Certified by the Federal Office for Information Security (BSI) in accordance with ISO 27001 on the basis of IT-Grundschutz | Certified in accordance with Payment Card Industry Data Security Standard (PCI DSS) | Qualified for critical infrastructure in accordance with §3 BSI Act | BSI C5 Type 2 | Certified Trusted Cloud Service | KRITIS operator in accordance with Section 8a (3) BSI Act