Politecnico di Torino
Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering
XXXV cycle

Supervisor
Prof. Riccardo Sisto
Dott. Fulvio Valenza

Network Security Automation

PhD Candidate: *Daniele Bringhenti*

1. Introduction and Motivation

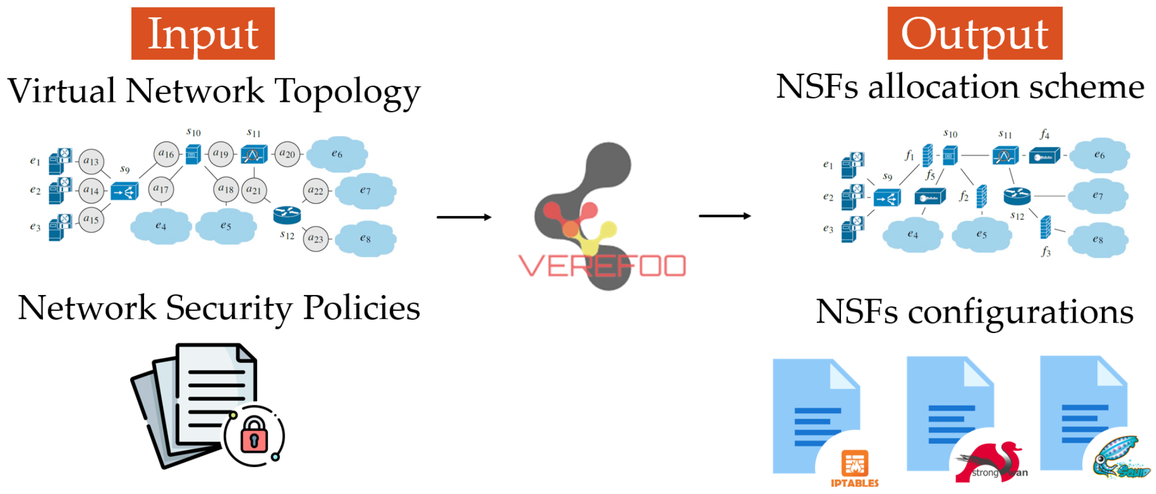
The upcoming evolution of computer networks towards virtualization has introduced flexibility and dynamicity, but at the same time it led to higher complexity. In this evolutionary environment, a manual orchestration and configuration of Network Security Functions (NSFs) is not feasible anymore, and it might cause countless unremarked breaches for cyberattacks.

2. The Proposed Solution

VEREFOO (VErified REFinement and Optimized Orchestration) is the first methodology in the literature that combines automation, formal verification and optimization for generating the allocation scheme and configuration of NSFs, so as to satisfy user-specified security policies [1].

VEREFOO pursues a "security by construction" approach, where formal assurance of the configuration correctness is provided without requiring a-posteriori verification. This is achieved by formulating the automatic configuration problem as a Maximum Satisfiability Modulo Theories (MaxSMT) problem, based on constraint programming. Formal models of virtual functions are included in VEREFOO [2], so as to capture all the required information for an automated security orchestration, without impacting on performance.

The MaxSMT problem formulation also enables the fulfillment of optimization criteria, e.g., the minimization of the configured rules to improve the efficiency of the NSF operations, and the optimization of reconfiguration transients [3].



3. Results and Future Work

The VEREFOO approach has been already applied to the auto-configuration of firewalls and VPN gateways, and an open-source implementation is available on GitHub [4]. The validation of this approach shows that it can scale up to networks composed of hundreds of nodes, under the specification of hundreds of security policies.

As future work, VEREFOO will be extended to support other NSF types (e.g., IDSs and anti-spam filters), and alternative heuristic algorithms will be explored.

4. References

1. D. Bringhenti, G. Marchetto, R. Sisto, F. Valenza, and J. Yusupov, "Automated firewall configuration in virtual networks", IEEE Transactions on Dependable and Secure Computing, 2022.
2. D. Bringhenti, G. Marchetto, R. Sisto, S. Spinoso, F. Valenza, and J. Yusupov, "Improving the formal verification of reachability policies in virtualized networks", IEEE Transactions on Network and Service Management, 2021.
3. D. Bringhenti and F. Valenza, "Optimizing distributed firewall reconfiguration transients", Computer Networks, Elsevier, 2022.
4. https://github.com/netgroup-polito/verefoo