DP2 – INTRODUCTION TO THE TOPIC OF THE ASSIGNMENTS – A.Y. 2016-17

The NF-FG concept

A Network Function-Forwarding Graph (NF-FG) describes a *network service* requested by an end-user from a Service Provider. An NF-FG models the requested network service as a graph, where the nodes represent network functions (e.g., firewall, NAT, etc.…), end-hosts, and servers composing the requested service, while the arcs represent packet forwarding paths.

Before deploying a requested service in her network, a Provider may want to verify the correctness of the service. An NF-FG verification service is in charge of checking whether an NF-FG satisfies a set of policies. A policy specifies a property of the network service.

In our exercise, an NF-FG is characterized by a name, which uniquely identifies it, and a set of Network Nodes. Each node has a name, which is unique within the NF-FG, and is associated to a "functional type" that must be present in the Provider's catalog. The catalog is fixed and includes the following types: firewall, DPI, NAT, anti-spam, web-cache, VPN gateway, web server, web client, mail server, and mail client. A node can be directly connected to a number of other nodes, by means of Links. A link represents a unidirectional connection between two nodes and is characterized by a name, which uniquely identifies it within the NF-FG, and the source and destination nodes of the connection.

A generic policy is characterized by a name, which uniquely identifies it, the NF-FG on which it has to be verified, and the result of its verification. A policy can be positive (if the property it represents must hold) or negative (if the property it represents must not hold).

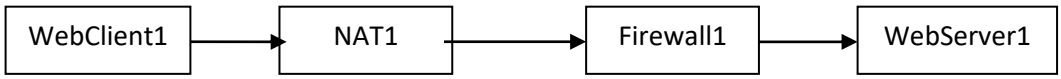
Two kinds of policy are considered: Reachability and Traversal policies. The first ones represent the existence of a path in the NF-FG that connects a source node to a destination node. Traversal policies instead are a specialization of reachability policies. The properties they specify can be expressed as follows: reachability must hold between a source node and a destination node and all the paths between the source and destination nodes must traverse a set of network functionalities. For example, we can specify that all the paths between node SRC and DST must pass through at least a firewall and a NAT.

The verification of a policy succeeds if the property associated with the policy is satisfied (or not satisfied in case of negative policy) by the NF-FG it points to. In this case, we say the policy is satisfied, otherwise we say it is violated. The verification service returns also a message that provides further details about the policy result and the time when the policy has been verified. If a NF-FG is updated, the policies correlated to it should be verified again. This situation can be detected because the verification time of a policy is before the NF-FG last update time.

NF-FG examples

Example 1

This is an example of NF-FG, described by the following picture (where network nodes are represented by rectangles containing their name, and the links from one node to another one are represented by arrows):

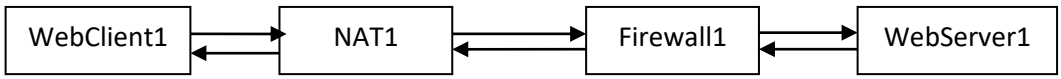


A set of possible policies for this example is the following:

Name	Type	SRCnode	DSTnode	Result	TraversedFunc.
Policy1	Reachability	WebClient1	WebServer1	Positive	-
Policy2	Reachability	WebServer1	WebClient1	Negative	-
Policy3	Traversal	WebClient1	WebServer1	Positive	Firewall

Example 2

Let us consider that the previous NF-FG has been updated as depicted in figure.



In this example, we expect the following verification results for the previous set of policies:

Name	Type	SRCnode	DSTnode	Result	TraversedFunc.
Policy1	Reachability	WebClient1	WebServer1	Positive	-
Policy2	Reachability	WebServer1	WebClient1	Positive	-
Policy3	Traversal	WebClient1	WebServer1	Positive	Firewall