Flow matrix guidelines UNDER CONSTRUCTION

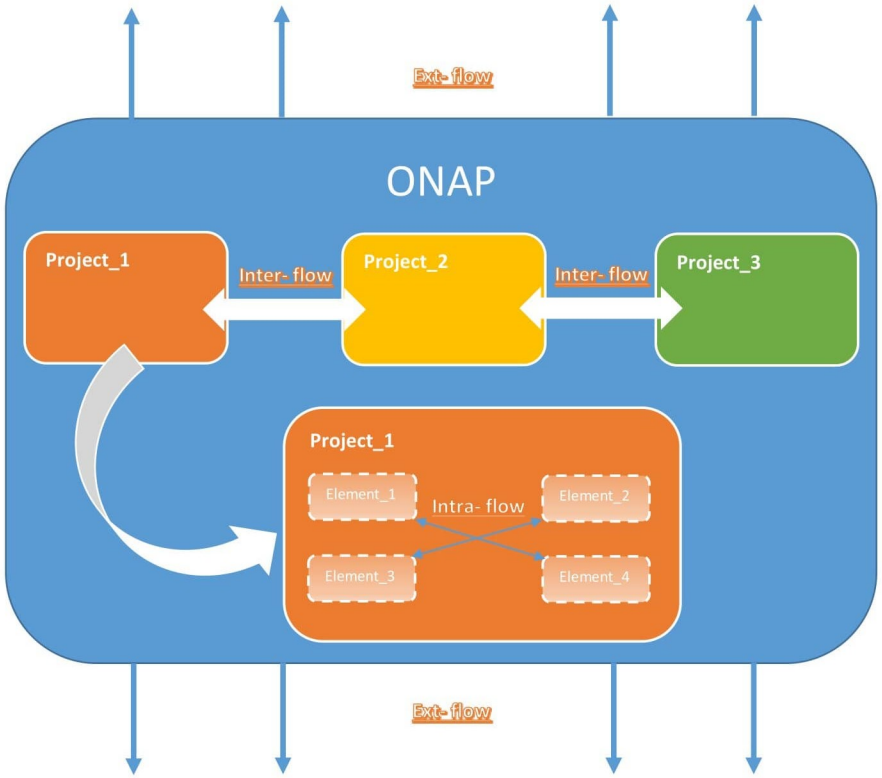
WHY a flow matrix?

Numerous components are embedded in the ONAP architecture.

To enable a reliable and efficient security level of the deployed solution, the owner of the solution has to manage his IN/OUT flows of it. Then adapted access control rules can be activated to enable only authorized incoming and outcoming flows.

Without this information, it is impossible to deploy a real **access control solution**.

For more clarity reasons, 3 types of flows have been defined.



- External flows

It is by definition all flows out of ONAP platforms e.g. interconnection to a BSS.

The main objective is then to authorize only pre configured flows on specific ports.

- Inter-components flows

All flows defined between components defined as project by ONAP.

For example it could concern a flow between the AAI and DCAE.

- Intra-component flows

The flows remain within the components - ONAP project.

For instance for DCAE component, a flow between the collector (VES) sub_component and DCAE_lifecycle_manager.

WHEN a flow matrix?

A flow matrix should be established for each ONAP project.

It should be reviewed at each major release of the component.

As all projects already exist:

1. first external flow should be specified.
2. then proceed with inter-components flows.
3. Intra-component flows

The 2 first steps are important to gather relevant information to build the **access control strategy** of ONAP platform.

The information regarding intra-component flows is interesting, but do not condition it.

HOW a flow matrix?

This may be too complicated to address all flows for a given project.

As a first step, external flows should be considered, and then the 2 other categories.

- a YAML file is available, in order to formalize the sharing of the information.: onap_matrix-flows.yaml

This file enables to provide information for each **external flow for the DCAE example**:

Parameter	Value
name	name of the ONAP project e.g. DCAE.
sub_components: - name:	real name of the sub component e.g. dcae-snmptrap-collector
external_server_side:	in external server side list only ingress (external -> ONAP) traffic
type:	nodePort
To_Be_Specified_communication:	This can be: 1. external_communication 2. inter-component_communication 3. intra-component_communication
description	e.g. SNMP trap
id	e.g. DCAE_EXT_1.
communication_initiator	which component initiates the communication. e.g. any component sending SNMP either internally to ONAP platform or externally e.g. xNF.
communication_receipt	which component is the dest of the communication.
protocol	at least level 4 or higher, to be specified if applicable.
version	to be specified if applicable
exposed_pod_port	to be specified if applicable
exposed_port	to be specified if applicable
encryption	none or active e.g. HTTPS implemented.
data_exchanged	specifies the file format, the main exchanged information. e.g. SNMP trap information.
tls_server	to specify whether the component hosts a TLS sever or a TLS client (yes or no), if applicable.
tls_client	to specify whether the component hosts a TLS sever or a TLS client (yes or no), if applicable.
flow_direction	incoming our outcoming.

==> This file has to be generated for each category: external, inter-components and intra-component flows.

AND WITH a flow matrix?

The YAML files will enable to dress a map of the different flows and then ports to be open and authorized for the running of the ONAP platform.

==> this enables a reliable and an efficient implementation of the access control.

A common repository is proposed, in order to have a central and common storage of the different files.

Project	Version	YAML : external_flows	YAML : inter_components_flows	YAML : intra_component_flows
DCAE				
AAI				
CLAMP				
MSB				
DMaaP				
SDC				
Policy				
Service Orchestrator				
OOF				
AAF				
logging				
APPC				
SDN-C				