SACM ECP Mapping

IETF 93

7/20/2015

Background

- Builds off of the Endpoint Compliance Standard I-D that introduces relevant IETF, ISO, and TCG specifications

- Demonstrate how the Endpoint Compliance Profile (ECP) can be used to achieve the SACM use cases

- Specifications in ECP contain IPR, but, the TCG has been willing to contribute specifications in the past

What is ECP?

- Application of NEA/TNC protocols and interfaces to monitor and securely exchange endpoint posture information

- Ensures endpoints are:
  - Uniquely identified
  - Authorized to be on the network
  - Running compliant software that is up-to-date

- Extensible to support other types of data

Specifications in ECP

- NEA (TNC): architecture to collect and securely exchange endpoint posture information
- IF-IMC / IF-IMV*: interfaces between IMCs and TNC Client / IMVs and TNC Server
- PA-TNC (IF-M): format for posture information messages and attributes to exchange posture information between IMCs and IMVs
  - SWID Message and Attributes for IF-M* provides the format to exchange SWID tags
- PB-TNC (IF-TNCCS): protocol to carry posture information messages between IMCs and IMVs
- PT-TLS / PT-EAP (IF-T): protocol to transport posture information between the NEA Client and Server using TLS / EAP
- Server Discovery and Validation*: locate and validate the trustworthiness of TNC Servers

* Would need to be contributed by the TCG

Mapping ECP to SACM use cases

- UC-1: define, publish, query and retrieve security automation data
  - Addressed in the descriptions of the other use cases
- UC-2: endpoint identification and assessment planning
  - An endpoint provides posture information to gain access to a network
  - Information is used for identification and targeting purposes
- UC-3: endpoint posture attribute value collection
  - Collection is triggered by various types of events including change in posture, new/updated guidance, periodic and ad-hoc reassessment requests, etc.
  - Posture information is used immediately and/or stored in a CMDB for later use
- UC-4: posture attribute evaluation
  - Analysis of collected posture information against the expected values
  - Result of analysis is used to initiate follow up actions

Why use ECP and NEA/TNC specifications in SACM?

- Addresses the major components of the SACM use cases
- They already exist and are available for us to use
- Avoids the creation of competing specifications which helps to unify the practice of endpoint posture assessment

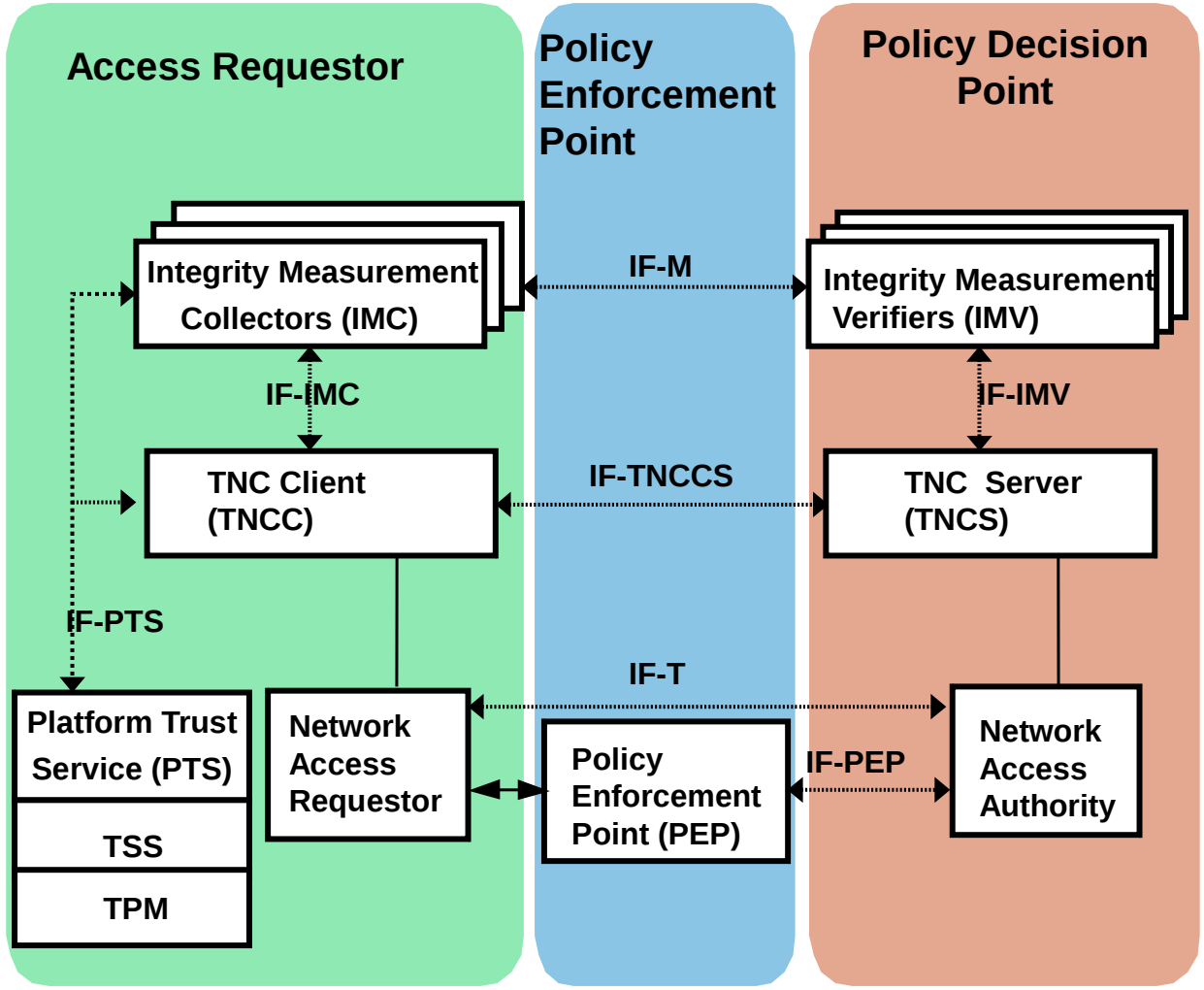
Next steps

- Determine if we want to use the IETF NEA and TCG TNC specifications

- If we decide to use the specifications:
  - Reach out to the TCG regarding the contribution of specifications
  - Update the architecture document to align with the IETF NEA architecture
  - Develop a roadmap for refining specifications to satisfy the needs of SACM

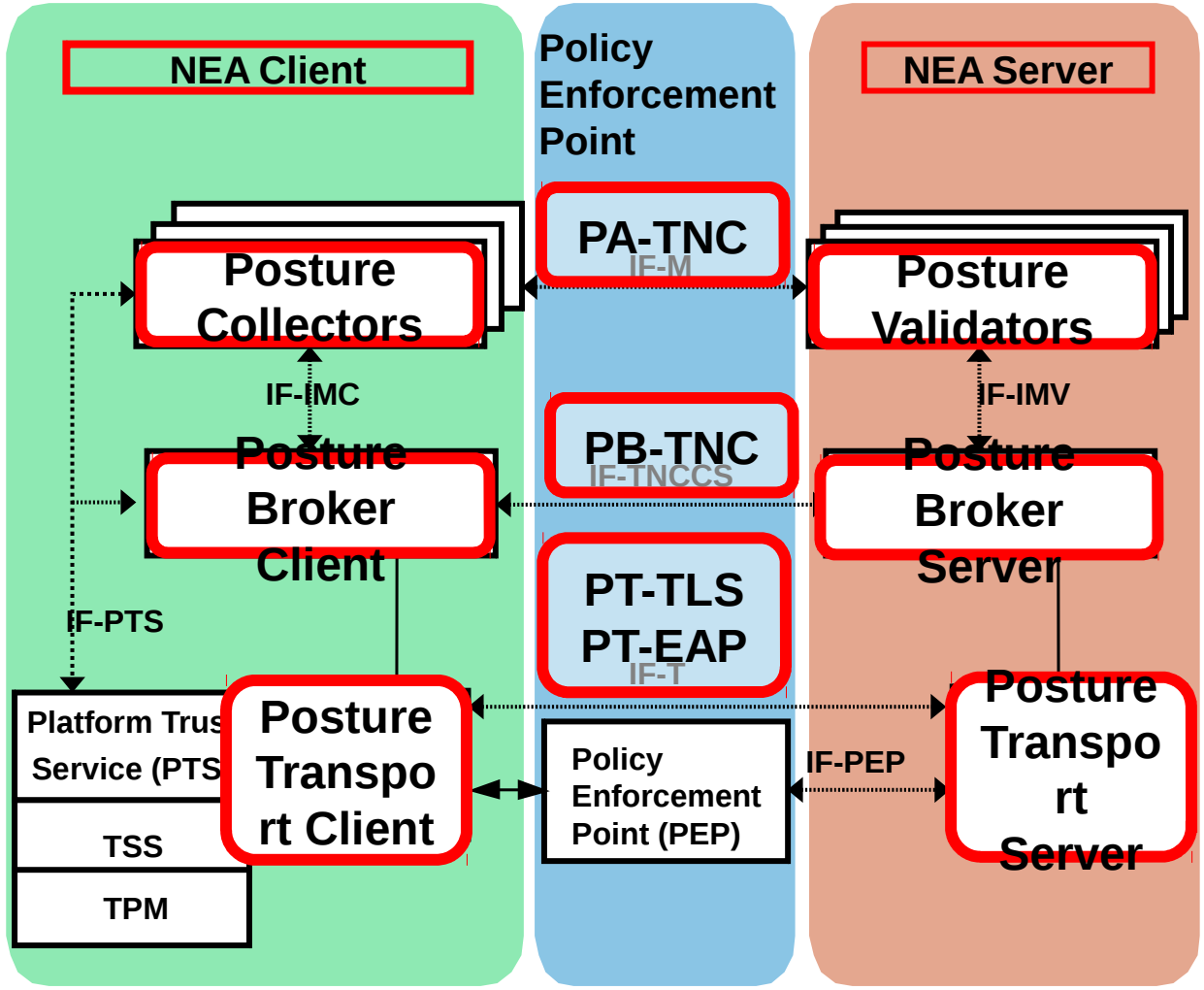
Back up slides

Quick refresher of the TNC architecture



http://www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications

Quick refresher of the TNC architecture



http://www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications