Endpoint Compliance Profile (ECP) FAQ
December 2014

Q. What is the Endpoint Compliance Profile?
A. The Endpoint Compliance Profile describes a profile of TNC standards and capabilities that is optimized to collect endpoint identity and posture attributes, and store this information in a searchable repository. This enables better awareness of the health of the entire enterprise by making it easier to perform analysis and investigation of the state of each endpoint. The ECP makes it possible to share collected data with authorized applications and users, enabling analysis and correlation of enterprise state both past and present. This allows the data to be more easily used for enterprise-wide asset management, threat defense, and security management.

Q. How does ECP fit within the TNC architecture?
A. The Endpoint Compliance Profile defines a refined set of requirements for TNC specifications, focusing on a specific subset of the TNC Architecture use cases but still using the TNC standard capabilities and schemas. It defines additional requirements for the TNC Architecture components to better support enterprise-wide awareness and management. Enterprises and implementers may continue to use the TNC Architecture and specifications without including the additional requirements added by the ECP if doing so meets their needs. However, enterprises that seek to develop a more comprehensive understanding of enterprise health may wish to consider the Endpoint Compliance Profile to better tune their TNC implementations to meet this need.

Q. Why is the Endpoint Compliance Profile important?
A. TNC users need to develop a comprehensive picture of enterprise health. The TNC Architecture has always allowed enterprises to analyze the state of endpoints and make access decisions based on the results, but the ECP goes beyond this by ensuring that certain types of information are always retrieved and then stored for later availability. Users of the Endpoint Compliance Profile know that they are getting a defined baseline of information about their endpoints expressed in a standardized format that allows network tools and administrators to make use of this information when making security, network-connectivity and asset management decisions. Sending this schema over TNC protocols means that the data is protected by secure, authorized network connections.

Q. Who has implemented the Endpoint Compliance Profile?
A. Although the ECP has just been published, it has already been by the highly-regarded strongSwan open source IPsec VPN solution. The source code for this implementation is available in a developer release at http://download.strongswan.org/strongswan-5.2.1rc1.tar.bz2 and a diagram showing how it works is available at http://www.strongswan.org/uml/testresults5dr/tnc/tnccs-20-pt-tls. Other parties are encouraged to consider experimental implementation of the ECP specifications so that feedback from these implementations can be used to improve the specifications before they are released in final form and widely implemented in products.

Q. What TNC specifications are affected by the Endpoint Compliance Profile?
A. The Endpoint Compliance Profile uses the TNC Access Requestor, Policy Decision Point, and the recently added Configuration Management Database. Towards this end it includes requirements for all TNC specifications that govern interactions within and between these components. Figure 1 below shows the components and interfaces addressed in the Endpoint Compliance Profile.

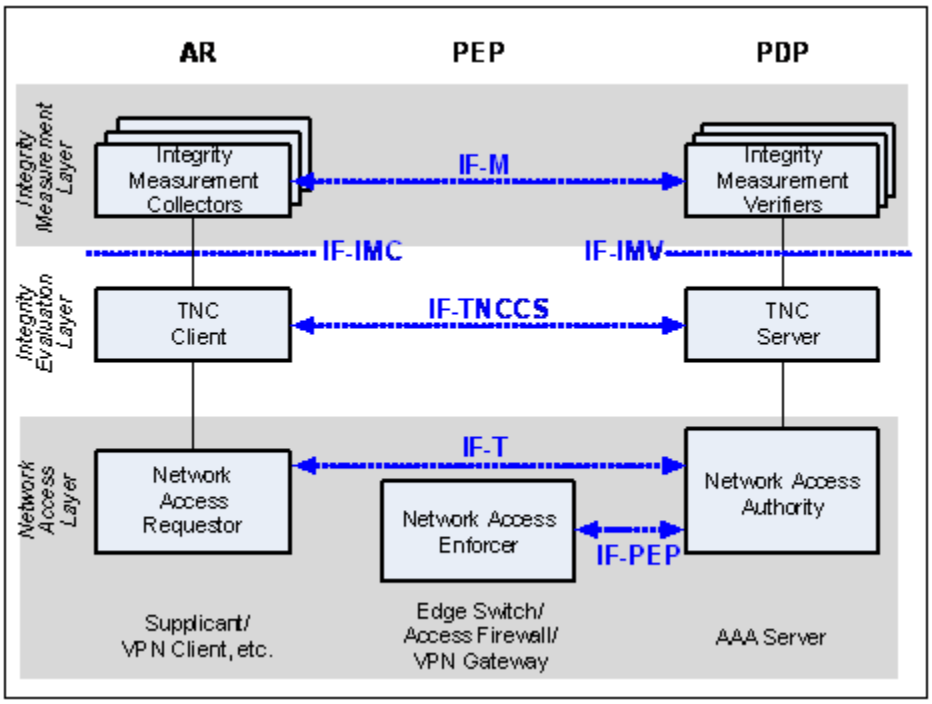

Figure 1 - TNC Architecture Covered by the Endpoint Compliance Profile

The Endpoint Compliance Profile does not currently include any requirements with regard to the Policy Enforcement Point (PEP), IF-MAP, or MAP Servers and Clients, and can be implemented in environments that do not contain either a PEP or a MAP implementation.

The Endpoint Compliance Profile adds one new component to the TNC architecture: the Configuration Management Database (CMDB). The CMDB interacts with the PDP and serves as a persistent repository for information collected from the enterprise's endpoints.

The Endpoint Compliance Profile was released in tandem with three additional TNC specifications. These specifications were created or updated to meet needs identified in the Endpoint Compliance Profile. However, in all cases, use of these new specifications does not require the use of the Endpoint Compliance Profile and they can all be used by implementations of the TNC Architecture that are not ECP-compliant. These specifications are:

- IF-IMV 1.4 (revision)
- PDP Server Discovery and Validation (new specification)
- SWID Message and Attributes for IF-M (new specification)

Q. What capabilities are added in the release of IF-IMV 1.4?
A. The 1.4 revision of the IF-IMV specification adds a standard way for TNCSs to expose information about endpoint identity to IMVs. The Endpoint Compliance Profile makes use of this to link collected data with the providing endpoint's identity, both during any immediate determination of endpoint compliance and when the information is added to the enterprise's long-term storage of collected information. Non-ECP implementations may make use of this to give IMVs the ability to include the identity of the endpoint in any determinations they make about endpoint compliance.

Q. What capabilities are added in the new PDP Server Discovery and Validation specification?

A. The PDP Server Discovery and Validation specification provides a way for an endpoint to discover a PDP to which it can report information and validate that this PDP is the correct entity to which it should be sending information. This can be used in situations where an endpoint has information to report regarding its state but does not currently have an existing connection to the PDP either because it joined the network without connecting to a PDP, or because its initial connection to the network was moderated by a PDP but the connection to the PDP was dropped after connectivity was granted. The Endpoint Compliance Profile includes requirements that endpoints report certain observed changes in their state to a PDP and, as such, endpoints need to be able to locate and validate a PDP if such a connection is not already being maintained. Non-ECP implementations may also make use of this to give endpoints a way to provide data to an enterprise's PDP regardless of whether that endpoint has an existing session with that PDP.

Q. What capabilities are added in the new SWID Message and Attributes for IF-M specification?

A. SWID tags are XML files that may be placed in a designated directory in an endpoint's file system when an application is installed. Because of this, one can look at the list of present SWID tags to get an indication as to which applications are present on an endpoint. The SWID Message and Attributes for IF-M specification standardizes how SWID tag information can be requested by an IMV and returned by an IMC. The Endpoint Compliance Profile requires that endpoints indicate their SWID tag collection to a PDP where it is passed to the CMDB for long-term storage. The ECP also requires that endpoints monitor their SWID tag collection and spontaneously report any observed changes to the PDP, thus allowing the CMDB information on the endpoint's SWID tag collection to remain up-to-date. Non-ECP implementations may also wish to make use of this specification if they wish to use an endpoint's SWID tag collection as part of the PDP's determination as to an endpoint's compliance with policy.