TCG Trusted Network Connect

Endpoint Compliance Profile

Specification Version 1
Revision 10
5 December 2014

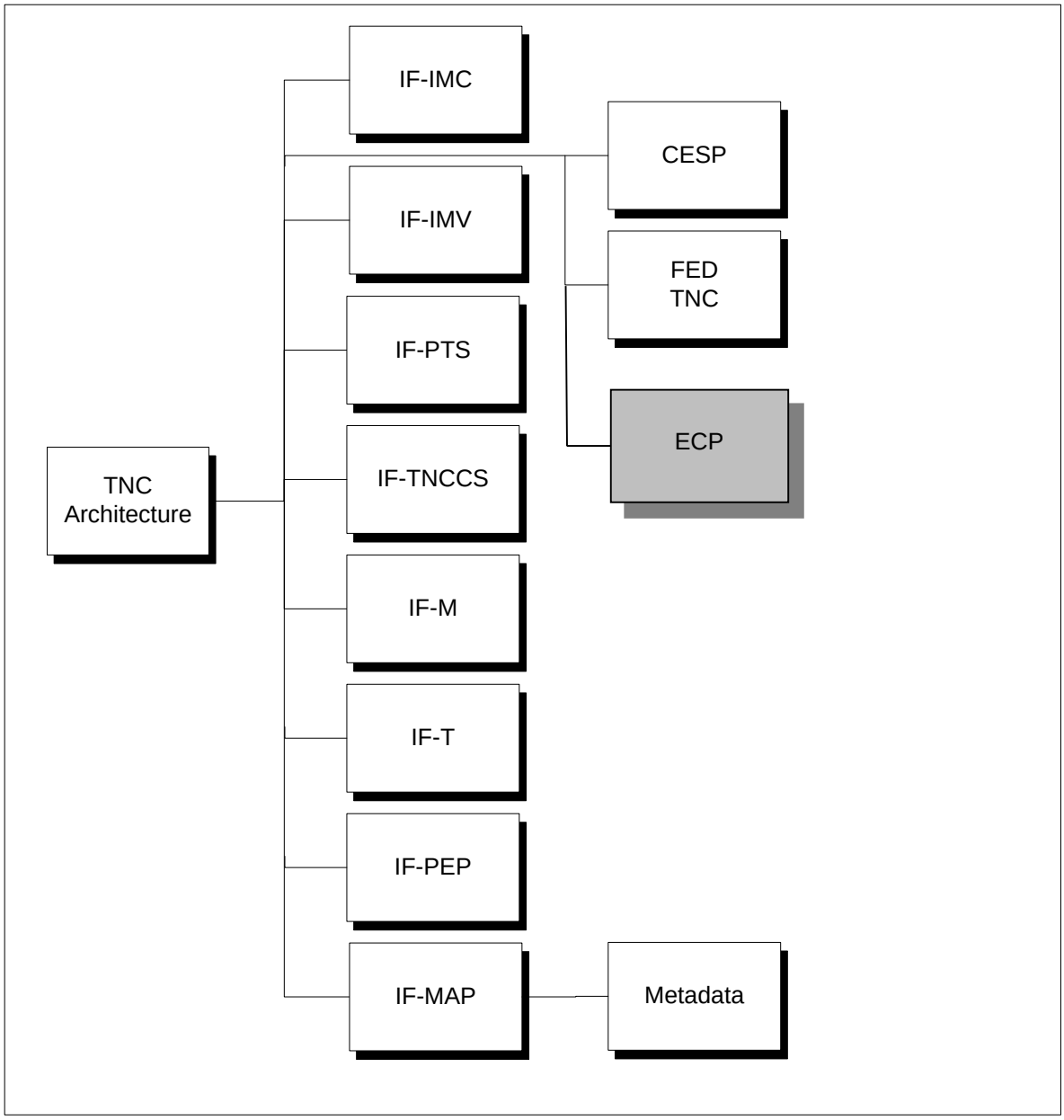
Contact:
admin@trustedcomputinggroup.org

TCG PUBLISHED

TCG

Disclaimer

TNC Document Roadmap



Acknowledgements

The TCG wishes to thank all those who contributed to this specification. This document builds on considerable work done in the various working groups in the TCG.

Padma Krishnaswamy	**Battelle Memorial Institute**
Eric Fleischman	**Boeing**
Richard Hill	**Boeing**
Steven Venema	**Boeing**
Nancy Cam-Winget	**Cisco Systems**
Scott Pope	**Cisco Systems**
Max Pritikin	Cisco Systems
Allan Thompson	**Cisco Systems**
Nicolai Kuntze	**Fraunhofer Institute for Secure Information Technology (SIT)**
Ira McDonald	**High North**
Dr. Andreas Steffen	**HSR University of Applied Sciences Rapperswil**
Josef von Helden	**Hochschule Hannover**
James Tan	**Infoblox**
Steve Hanna (TNC-WG Co-Chair)	**Juniper Networks**
Cliff Kahn	**Juniper Networks**
Lisa Lorenzin	**Juniper Networks**
Atul Shah (TNC-WG Co-Chair)	**Microsoft**
Jon Baker	**MITRE**
Charles Schmidt	**MITRE**
Rainer Enders	**NCP Engineering**
Dick Wilkins	**Phoenix Technologies**
David Waltermire	**NIST**
Mike Boyle	**U.S. Government**
Emily Doll	**U.S. Government**
Jessica Fitzgerald-McKay (Editor)	**U.S. Government**
Mary Lessels	**U.S. Government**
Chris Salter (Editor)	**U.S. Government**

Table of Contents

1 Introduction 8
1.1 Preventative Compliance Checks 8
1.2 Standardized Schema 9
1.3 Secure, Standardized Protocols 9
1.4 Keywords 10
2 Endpoint Compliance Profile Overview 11
2.1 Compliance Checking 11
2.2 Data Storage 11
2.3 Remediation 11
2.4 Future Work 11
3 Background 13
3.1 Role of the Endpoint Compliance Profile 13
3.2 Supported Use Cases 13
3.2.1 Connected and Compliant 13
3.2.2 Exposing Data to the Network 14
3.3 Non-supported Use Cases 15
3.4 Profile Requirements 15
3.5 Assumptions 16
4 Endpoint Compliance Requirements 19
4.1 Endpoint Pre-Provisioning 19
4.1.1 SWID Tags 19
4.1.2 Device Identity and Machine Certificate 19
4.2 Verifiers and Collectors 19
4.2.1 SWID Collectors and Verifiers 19
4.3 TNC Client and Server 20
4.3.1 TNCC 20
The TNCC MUST also conform to [IF-IMC] to enable communications with the SWID Collector. 20
4.3.2 TNCS 20
4.4 Configuration Management Database (CMDB) 20
4.5 Network Access Requestor (NAR) and Network Access Authority (NAA) 21
4.6 Administrative Interface and API 21
5 Security Considerations 22
5.1 Security Benefits of Endpoint Compliance Profile 22
5.2 Threat Model 23
5.2.1 Endpoint Attacks 23
5.2.2 Network Attacks 24
5.2.3 PDP Attacks 24
5.2.4 CMDB Attacks 24
5.3 Countermeasures 24
5.3.1 Countermeasures for Endpoint Attacks 25
5.3.2 Countermeasures for Network Attacks 25
5.3.3 Countermeasures for PDP Attacks 25
5.3.4 Countermeasures for CMDB Attacks 25
6 Privacy Considerations 27
7 Endpoint Compliance Profile Examples 28
7.1 Continuous Monitoring of an Endpoint 28
7.1.1 Change on Endpoint Triggers Compliance Report 28
7.2 Network Administrator Searches for Vulnerable Endpoints 29
8 Appendix A: Comply to Connect 31
8.1 Comply-to-Connect Use Case 31
8.2 Comply-to-Connect Requirements 32
8.2.1 IF-M Collectors and Verifiers 32

8.2.2 The Network Access Requestor (NAR) and Network Access Authority (NAA) 32
8.2.3 Policy Enforcement Point (PEP) 32
8.2.4 Administrative Interface 32
9 References 33
9.1 Normative References 33
9.2 Informative References 33

1 Introduction

The Trusted Network Connect Work Group (TNC-WG) has defined an open architecture for network security, including standard protocols for endpoint assessment and remediation. The Endpoint Compliance Profile (ECP) builds on the TNC protocols and interfaces to determine the compliance status of any type of endpoint on a network. The first generation of this specification focuses on reducing the security exposure of a network by confirming that all endpoints are:

- uniquely identified;
- authorized to be on the network; and
- running compliant software.

The TNC and the IETF define an endpoint as any network-connected device. Therefore, the Endpoint Compliance Profile standardizes the collection of endpoint health and state reports - hereafter referred to as "compliance reports" - from all types of endpoints, including user devices, servers, and infrastructure.

When ECP is used, compliance information is gathered by the TNC client running on the endpoint and is forwarded to the TNC server, which stores it in a Configuration Management Database (CMDB). This information is gathered while the endpoint is already connected to the network. The TNC server will likely be running on a PDP dedicated to compliance. Administrators will query the CMDB to determine the compliance status of an endpoint. For example, if a vulnerability is discovered in a product, an administrator may query the CMDB to determine which endpoints have the vulnerable software and thus need remediation.

Future versions of the ECP will address how to expose information—such as endpoint roles, the software that is supposed to be running on an endpoint, and the activities an endpoint is supposed to be performing—to network sensors that are looking for indicators of attacks and malicious activity on the network.

1.1 Preventative Compliance Checks

The value of preventative compliance checking is well established. Network security experts have for years identified software updating and patching as a critical step for preventing network intrusions. Application white listing, patching applications and operating systems, and using the latest versions of applications top the Defense Signals Directorate's "Top 4 Mitigations to Protect Your ICT System". [DSD] "Inventory of Authorized and Unauthorized Devices", "Inventory of Authorized and Unauthorized Software", and "Continuous Vulnerability Assessment and Remediation" are Critical Controls 1, 2, and 4, respectively, of the SANS "20 Critical Security Controls". [SANS] While there are commercially available solutions that attempt to address these network security controls, these solutions do not run on all types of endpoints; consistently interoperate with other network tools that could make use of the data collected; collect compliance reports from all types of endpoints in a consistent, standardized schema; or require vetted, standardized protocols that have been evaluated by the international community for cryptographic soundness.

As is true of most compliance solutions offered today, the solution found in the ECP does not attempt to solve the lying endpoint problem. A machine that has already been infected with malicious software can make false reports on its identity and the software it is running. The primary purpose of the ECP is not to detect infected machines; rather, it focuses on *ensuring that healthy machines remain healthy* by keeping software up-to-date and patched. The first goal of the ECP is to help an administrator be able to readily determine which endpoints that need remediation. Future versions of the ECP will address how to expose compliance information to network sensors to aid detection of attacks and remediation of endpoints.

1.2 Standardized Schema

The ECP requires the use of standardized schema for the exchange of compliance reports. This helps to ensure that the compliance reports sent from endpoints to the CMDB can be easily stored, due to their known format, and shared with authorized machines and users. Standardized schema also enable collection from myriad types of endpoints. Such standardization saves implementers time and money—time that does not have to be spent integrating new schema into the network's reporting mechanisms, and money that does not have to be spent on developing tools to parse information from each type of endpoint connected to the network. Standardized schema also enable the development of standardized client software. This allows endpoint vendors to include their own client software that can interoperate with compliance infrastructure and thus not have to introduce third party code onto their devices.

1.3 Secure, Standardized Protocols

Compliance reports must be sent over mature, standardized protocols to ensure the confidentiality and authenticity of this data while in transit. The ECP requires use of the IF-T Binding to TLS protocol for communication between the endpoint and the Policy Decision Point (PDP). (As noted above, the PDP is likely to be a device dedicated to compliance). This protocol allows networks that implement this solution to collect large amounts of information from an endpoint in order to make decisions about that endpoint's compliance to network policy. This Profile offers a compliance solution for all endpoints—including endpoints already connected to the network, as well as those seeking to join the network for the first time. Periodic compliance checks and automated reporting of changes to installed software allow for instantaneous identification of connected devices that are no longer compliant to network policy.

The Trusted Network Connect Work Group has designed an architecture to support endpoint compliance reporting. Figure 1 illustrates the architectural components used in the Endpoint Compliance Profile:

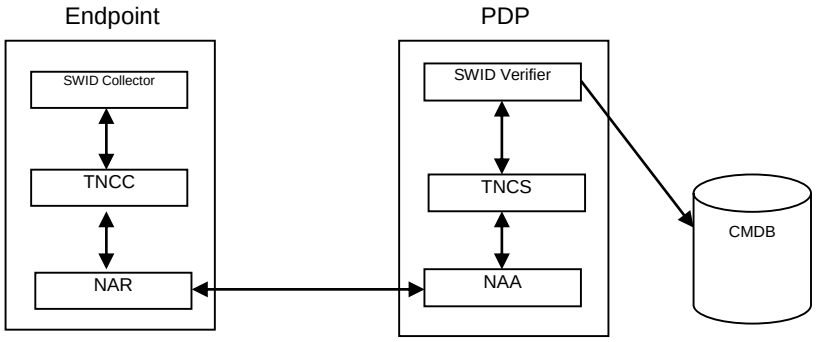


Figure 1: The Endpoint Compliance Architecture

Note that the SWID Collector and SWID Verifier are implementations of TNC's IMC and IMV architectural components, respectively. Requirements for each of the components in the diagram above are contained in this profile. The reader should consult [TNC Architecture] for additional information on these components. All current CMDB requirements are contained within the Endpoint Compliance Profile.

The TNC Architecture defines requirements for the Policy Decision Point that include a RADIUS server. This is necessary for the comply-to-connect use case; however, this is not a requirement for the PDP used in the Endpoint Compliance Profile. The PDP as described in this document is responsible for gathering the information reported by the endpoints and storing the data in the CMDB. RADIUS functionality, if desired, may be implemented either on the PDP as described in this document, or separately in the network architecture.

1.4 Keywords

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC 2119]0. This specification does not distinguish blocks of informative comments and normative requirements. Therefore, for the sake of clarity, note that lower case instances of must, should, etc. do not indicate normative requirements.

2 Endpoint Compliance Profile Overview

The Endpoint Compliance Profile describes how TNC specifications can be used to support compliance checking and remediation of endpoints on a network. This profile does not generate new schema or protocols; rather, it offers a full end-to-end solution for compliance checking, as well as a fresh perspective on how existing standards can be leveraged against network vulnerabilities.

2.1 Compliance Checking

The Endpoint Compliance Profile 1.0 describes how TNC specifications make it possible to perform compliance checks against all network-connected devices by:

1. uniquely identifying the endpoint;
2. collecting and assessing compliance based on data from the endpoint;
3. creating a secure, authenticated, confidential channel between the endpoint and the Policy Decision Point (PDP);
4. enabling the endpoint to notify the PDP about changes to its configuration;
5. enabling the PDP to request information about the configuration of the endpoint; and
6. storing the configuration information in a database linked to the identifier for the endpoint.

2.2 Data Storage

The ISO/IEC Software Identification Tag standard [SWID] has defined a schema for identifying applications installed on endpoints and their patch status. The Endpoint Compliance Profile 1.0 focuses on being able to collect this information from an endpoint and store it in a Configuration Management Database (CMDB). This makes compliance data from a network's endpoints available to authorized network infrastructure and network administrators. Uses of this data are innumerable—asset management solutions, analytics tools, gateway devices that need to make additional connectivity decisions, and metrics reporting scripts, among others, are all able to reference the data stored in the CMDB to achieve their purposes.

2.3 Remediation

The ability of the TNC client to notify the PDP whenever a modification is made to the endpoint enables immediate identification of endpoints that need remediation. The Endpoint Compliance Profile 1.0 does not specify requirements for remediation. However, TNC specifications do support the ability to send quarantine and disconnect instructions to the PEP enforcing access control for a non-compliant endpoint. For those wishing to integrate such capabilities into their Endpoint Compliance solution, requirements for this TNC scenario can be found in Appendix A.

There is a clear need for nuanced, automated remediation instructions sent from the PDP to the endpoint (for example, to update an endpoint's software, or remove a piece of non-compliant software). Those messages are complicated to define and may have to be tailored to a particular operating system. Future versions of this specification may address which instructions can be defined based on the configuration content that is collected from endpoints.

2.4 Future Work

Future generations of the TNC Endpoint Compliance Profile will incorporate other types of data available from endpoints, such as configuration settings, when suitable schema are developed and are supported by vendors.

TNC-WG intends to develop a formal interface to the CMDB that will allow other security automation applications a standardized interface to tap into the information gathered for compliance from the endpoints.

Future versions of this specification will address which remediation instructions can be defined based on the configuration content that is collected from endpoints.

The TNC-WG intends to formalize the functions required in a PDP administrative interface to support policy-based decisions on whether an endpoint is compliant to network policy.

An implementer who chooses to use a compliance-dedicated PDP as described in the ECP may wish to integrate a RADIUS-based PDP on their network as well. Full integration of the two PDPs may require the ECP's SWID Verifier to communicate with the TNCS on the RADIUS-based PDP.

3 Background

3.1 Role of the Endpoint Compliance Profile

The Endpoint Compliance Profile describes a standard way to communicate endpoint identity and endpoint state and health information such as software identity and software version to a Policy Decision Point, and to make this compliance data available to other authorized pieces of infrastructure. The Endpoint Compliance Profile 1.0 focuses on collecting the application information available in SWID tags, as specified in [SWID]; later versions will expand on the information collected, as described in the “Future Work” section of this profile.

3.2 Supported Use Cases

The Endpoint Compliance Profile focuses on compliance checks on enterprise devices on enterprise networks. Use cases supported by the Endpoint Compliance Profile 1.0 are as follows:

3.2.1 Connected and Compliant

A network-connected endpoint sends compliance data using the SWID Messages for IF-M and other standard schemas over TNC protocols.

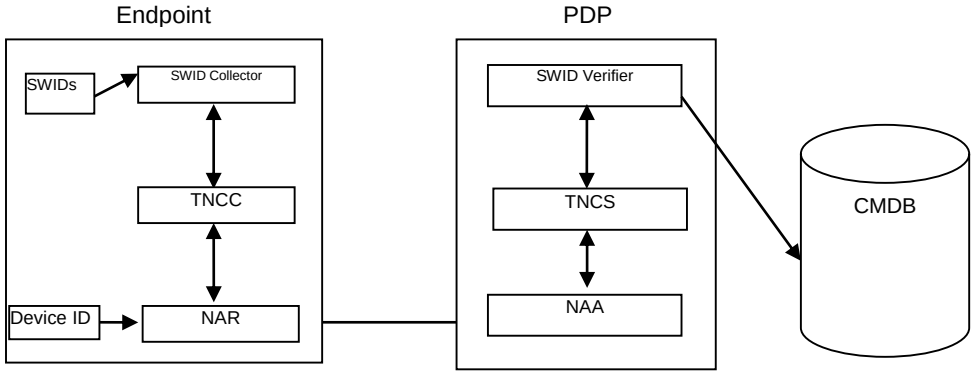


Figure 2: Connected and Compliant Use Case

1) If necessary, the endpoint finds and validates the Policy Decision Point (PDP) in compliance with [PDP Discovery and Validation].

2) The Network Access Requestor (NAR) on the endpoint and Network Access Authority (NAA) on the PDP complete a TLS handshake, during which endpoint identity information is exchanged.

3) Either the TNC Server (TNCS) on the PDP or the TNC Client (TNCC) on the endpoint initiates a compliance check. Checks may be triggered for multiple reasons, including:

a) network policy states that a previous check has aged out and become invalid;

b) the TNCC notices that the relevant compliance data on the endpoint has changed, (for example, due to application updates, deletions or additions); or

c) the TNCS is alerted by a network sensor or an administrator (via the PDP’s user interface) that a check must be completed.

All information exchanges between the collectors and verifiers are subject to the network's policy, which may limit the content or size of information sent between the endpoint and the PDP.

4) The SWID Collector on the endpoint collects from the SWID tag repository on the endpoint. This data is sent via the TNC Client (TNCC) and NAR to the PDP.

5) Once the compliance report is received by the NAR, it is forwarded to the SWID Verifier via the TNCS. The SWID Verifier also forwards the data to the Configuration Management Database (CMDB). The report is stored along with past compliance data collected about the endpoint.

3.2.2 Exposing Data to the Network

Because the endpoint compliance report was sent in a standards-based schema (ISO/IEC 19770-2:2009) over secure, standardized protocols (IF-T TLS), and the SWID tags are stored in a centralized location (the CMDB) linked to unique endpoint identifiers, authorized users are able to access the report. Such authorized users may include, but are not limited to, a network administrator or network owner (via the PDP's administrative interface), and other pieces of infrastructure that can make use of this data (via the PDP's API). The PDP will provide:

- a standard administrative interface that allows data sharing with authorized users and administrators;
- a standard API that allows data sharing with authorized infrastructure and software;
- a persistent account of endpoints that have connected to the network over a period of time set by the administrator;
- the identities provided by those endpoints; and
- what SWIDs were reported by the endpoint.

The endpoint will report updates as its local SWID repository changes, as well as each time it disconnects and reconnects to the network.

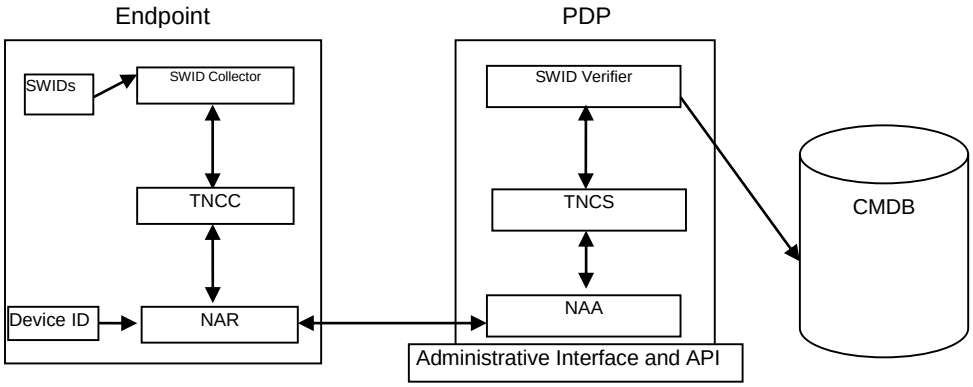


Figure 3: Exposing Data to the Network

3.2.2.1 Asset Management

Using the administrative interface on the PDP, an authorized user can learn:

- what endpoints are connected to the network at any given time; and
- what SWID tags were reported for the endpoints.

The ability to answer these questions offers a standards-based approach to asset management and asset reporting, which is a vital part of enterprise tasks such as compliance report generation for FISMA, PCI, HIPAA, etc.

3.2.2.2 Vulnerability Searches

The administrative interface also provides the ability for authorized users or infrastructure to locate endpoints running software for which vulnerabilities have been announced. Because of

1. the unique IDs assigned to each device; and
2. the rich application data provided in the devices' compliance report,

the CMDB can be queried to find all devices running a vulnerable application. Devices suspected of being vulnerable can be remediated by the network administrator or flagged for further scrutiny.

3.2.2.3 Threat Detection and Analysis

The CMDB's standardized API allows authorized infrastructure devices and software to search endpoint compliance reports for evidence that an endpoint's software inventory has changed, and can make endpoint software inventory data available to other network access control devices. This automates security data sharing in a way that expedites the correlation of relevant network data, allowing administrators and infrastructure devices to identify odd device behavior and configuration using secure, standards-based schema and protocols.

3.3 Non-supported Use Cases

Several use cases, including but not limited to these, are not covered by the Endpoint Compliance Profile 1.0:

- Gathering other types of compliance data

  The Endpoint Compliance Profile does not prevent network administrators from collecting other types of compliance data other than SWIDs from the endpoint; however it does not set requirements for doing so.

- Solving the lying endpoint problem

  The Endpoint Compliance Profile does not address the lying endpoint problem; that is, the Profile makes no assertions that it can catch an endpoint that is, either maliciously or accidentally, reporting false information to the PDP. However, other network security solutions may be able to use the information collected using the capabilities described in this profile to catch an endpoint in a lie. For example, a network sensor may be able to compare the information it has collected on an endpoint's activity on the network to what the endpoint reported to the PDP and flag discrepancies. However, these particular capabilities are not described in this profile.

- Publish/subscribe CMDB interface

  Future versions of the Endpoint Compliance Profile may specify a publish/subscribe interface for the CMDB, so infrastructure device can subscribe to and receive published reports from the CMDB regarding endpoint configuration changes. However, the Endpoint Compliance Profile 1.0 includes no such requirements.

3.4 Profile Requirements

Here are the requirements that the Endpoint Compliance Profile protocol must meet in order to successfully play its role in the TNC architecture.

- **Meets the needs of the TNC architecture**
  The Endpoint Compliance Profile must support all the functions and use cases described in the TNC architecture as they apply to endpoint compliance reporting.

- **Efficient**
  In the comply-to-connect use case, the TNC architecture delays network access until endpoint privileges are determined based on local access control configuration. To minimize user frustration, it is essential to minimize delays by making Endpoint Compliance comply-to-connect health checks as brief and efficient as possible, and completing more robust health checks after the endpoint has an IP address.

- **Extensible**
  The Endpoint Compliance Profile needs to expand over time as new features are added to the TNC architecture. The solution must allow new features to be added easily, providing for a smooth transition and allowing newer and older architectural components to continue to work together. Further, the Endpoint Compliance Profile and the specifications referenced here must define safe extensibility mechanisms that enable innovation without breaking interoperability.

- **Easy to implement**
  The Endpoint Compliance Profile should be easy for vendors to implement in their products, and should result in products that are easy for network administrators to implement on their networks. Products conformant to the Endpoint Compliance Profile should interoperate seamlessly, and be simple to integrate into existing network infrastructure.

- **Easy to use**
  The Endpoint Compliance Profile should describe a simple, integrated user interface that network administrators can use to perform the tasks listed in the profile's use cases. The Endpoint Compliance Profile should not constrain innovation by specifying details of the user interface but rather functional requirements.

- **Platform-independent**
  Since network environments may contain many different types of endpoints, the solution should function independently of the endpoint platform.

- **Scalable**
  The Endpoint Compliance Profile must be designed to scale to very large numbers of endpoints.

3.5 Assumptions

Here are the assumptions that the Endpoint Compliance Profile makes about other components in the TNC architecture.

- **Existence of PDP and CMDB**
  The Endpoint Compliance Profile assumes that a PDP and CMDB exist. A PEP is not required for the implementation of this solution.

- **Endpoint SWID installation**
  The Endpoint Compliance Profile assumes that an endpoint has been pre-provisioned with Software Identification Tags for its applications, and that these SWID tags are formatted and stored in conformance with [SWID].

- **Certificate provisioning**
  In order to implement the most secure device identification option, the Endpoint Compliance Profile assumes that the enterprise has set up a certificate root authority, and has provisioned each endpoint with a device identification certificate. This is not required if an enterprise chooses to use other device authentication methods.

In addition, the Endpoint Compliance Profile makes the following assumptions about the compliance ecosystem:

- **All network-connected devices are endpoints**

  As defined by [RFC 5209] Section 2, an endpoint is any computing device that can be connected to a network. Compliance checking against network policy is equally, if not more, important for continuously connected devices, such as enterprise PCs and infrastructure devices, as it is for sporadically connected devices that are often the subject of BYOD or comply-to-connect specifications. Continuously connected devices are just as likely to fall out of compliance with network policy, and a standardized compliance checking method is necessary to ensure they can be properly remediated.

- **All endpoints on the network must be uniquely identified**

  Many enterprise network administrators struggle to identify what endpoints are connected at any given time. By requiring a standardized method of endpoint identity, the Endpoint Compliance Profile will enable administrators to answer the basic question, “What is on my network?”

  Unique device identification also enables the comparison of current and past endpoint compliance reports, by allowing administrators to correlate reports from the same endpoint. This makes it easier to flag suspicious changes in endpoint configuration for manual or automatic review, and helps to swiftly identify malicious changes to endpoint applications.

- **Compliance checks must occur over secure, standardized protocols**

  Endpoint identity and application information is very valuable, both to network administrators and to network attackers. Therefore, it must be kept confidential, using secure protocols to transport it from the endpoint to network infrastructure devices. Additionally, it is critical that only authorized parties be capable of requesting information, receiving information, or taking action to change an endpoint's connectivity status.

  Relying on standardized protocols to provide this security enables greater interoperability and compatibility between devices, and allows for the development of compliance testing to ensure that each device operates securely and in conformance with appropriate specifications. A standards body provides a process for experts in protocols and cryptography to evaluate the soundness of protocols and security management procedures; a set of security standards allows an enterprise to make the most effective use of their investment in a security management infrastructure.

- **Compliance reports must be formatted using standardized schema**

  Well-known, standard schema allow for a universal language for compliance reporting. With each endpoint speaking the same language, the Endpoint Compliance Profile enables information sharing between user endpoints and infrastructure devices, and between infrastructure devices that perform different network security tasks.

- **Compliance data must be stored by the CMDB and must be exposed to an interface at the PDP**

  A standard schema enables standard queries from an interface exposed to an administrator at the PDP console. A database must retain any current compliance information retrieved from the endpoint and store it indexed by the unique identifier for the endpoint. Any verifier

specified by this profile must be able to ascertain from its corresponding collector whether the compliance data is up to date. An interface on the PDP must support a request to the verifier to obtain up to date information when an endpoint is connected. This interface must also support the ability to make a standard set of queries about the compliance information stored by the CMDB.

In the future, some forms of compliance data might be retained at the endpoint. The interface on the PDP must accommodate the ability to make a request through the verifier to the corresponding collector about the health or compliance state of the endpoint.

Standard schema and protocols also enable the security of compliance reports. By storing these reports indexed under the endpoint's unique identification, secure storage itself enables endpoint data correlation, and ensures that the network's databases always offer the freshest, most up-to-date view of the network's compliance state possible

- **Compliance data can be shared with the network**
  By exposing compliance data using a standard interface and API, other security and operational components have a high level of insight into the network's endpoints and the software installed on them. This will support innovation in the areas of asset management, vulnerability scanning, and administrative interfaces, as any authorized infrastructure device can interact with the data.

- **Network owners and administrators must have complete control of compliance data, network policy, and endpoint mitigation**
  Enterprise asset compliance data belongs to the enterprise. Standardized schema, protocols and interfaces help to ensure that this data is not locked in proprietary databases, but is made available to its owners. This enables administrators to develop as nuanced a policy as necessary to keep their networks secure.

4 Endpoint Compliance Requirements

These requirements are written with a view to performing a compliance check on a conventional end user device; as the Endpoint Compliance Profile grows and evolves, these requirements will be expanded to address issues that arise for performing compliance checking on other types of endpoints. Note that these requirements refer to defined components of the TNC architecture. As with the TNC architecture, implementers have discretion as to how these TNC components map to separate pieces of software or devices.

4.1 Endpoint Pre-Provisioning

The following requirements assume that the platform or OS vendor supports the use of SWID tags and has identified a standard directory location for the SWID tags to be located as specified by [SWID].

4.1.1 SWID Tags

The primary content for the Endpoint Compliance Profile 1.0 is the information conveyed in the elements of a SWID tag.
The endpoint MUST have SWID tags stored in a directory specified in [SWID]. The tags SHOULD be provided by the software vendor; they MAY also be generated by

- the software installer; or
- third-party software that creates tags based on the applications it sees installed on the endpoint.

The elements in the SWID tag MUST be populated as specified in [SWID]. These tags, and the directory in which they are stored, MUST be updated as software is added, removed, or updated.

4.1.2 Device Identity and Machine Certificate

The endpoint SHOULD authenticate to the PDP using a machine certificate during the establishment of the outer tunnel achieved with IF-T. [IF-IMV] specifies how to pull an endpoint ID out of a machine certificate. An endpoint ID SHOULD be created in conformance with [IF-IMV] from a machine certificate sent via [IF-T TLS] or [IF-T Tunneled EAP].
In the future, the identity could be a hardware certificate compliant with [IEEE 802.1ar]; ideally, this ID SHOULD be associated with the identity of a TPM if present on the endpoint.
The enterprise SHOULD stand up a certificate root authority; install its root certificate on endpoints and on the PDP; and provision the endpoints and the PDP with machine certificates.
The endpoint MAY authenticate to the PDP using a combination of the machine account and password; however, this is less secure and not recommended.

4.2 Verifiers and Collectors

Any collector used in an Endpoint Compliance Profile solution MUST be conformant with [IF-IMC].
Any verifier used in an Endpoint Compliance Profile solution MUST be conformant with [IF-IMV].

4.2.1 SWID Collectors and Verifiers

4.2.1.1 The SWID Collector

For the Endpoint Compliance Profile, the SWID Collector MUST be conformant with [SWID Messages for IF-M], which includes requirements for:

1. Collecting SWID tags from the SWID directory
2. Monitoring the SWID directory for changes
3. Initiating a session with the PDP to report changes to the directory
4. Maintaining a list of changes to the SWID directory when updates take place and no IF-T TLS connection can be created with the PDP

5. Responding to a request for SWID tags from the SWID verifier on the PDP
6. Responding to a query from the SWID verifier as to whether all updates have been sent

The SWID Collector is not responsible for detecting that the SWID directory was not updated when an application was either installed or uninstalled.

4.2.1.2 The SWID Verifier

Conformance to [SWID Messages for IF-M] enables the SWID Verifier to:

1. Send messages to the SWID collector (at the behest of the administrator at the PDP console) requesting updates for SWID tags located on endpoint
2. Ask the SWID Collector whether all updates to the SWID directory located at the PDP have been sent (this message helps establish whether information is up to data when a client attempts to connect with IF-T over EAP)
3. Compare an endpoint's SWID report to network policy, and make a recommendation to the TNC Server about the endpoint's continued connectivity

In addition to these requirements, a SWID Verifier used in conformance with this profile MUST be capable of passing information from the compliance reports and the endpoint identity associated with that report to the CMDB for storage.

4.3 TNC Client and Server

[IF-TNCCS] describes a standard way for the TNC Client (TNCC) and the TNC Server (TNCS) to exchange messages.

4.3.1 TNCC

The TNCC MUST conform to [IF-TNCCS], which levies a number of requirements against the TNCC. A TNCC that complies with these requirements will be able to:

1. attempt to initiate a session with the TNCS if the SWID Collector makes a request to send an update to the SWID directory to the PDP;
2. notify the SWID Collector if no IF-T TLS session with the PDP can be created;
3. notify the SWID Collector when an IF-T TLS session is established; and
4. receive information from the IMCs, forward this information to the PDP via the NAR.

The TNCC MUST also conform to [IF-IMC] to enable communications with the SWID Collector.

4.3.2 TNCS

The TNCS MUST conform to all requirements in the [IF-TNCCS] and [IF-IMV] specifications. Conformance to [IF-IMV] enables the TNCS to obtain endpoint identity information from the NAA, and pass this information to any IMVs on the PDP.

4.4 Configuration Management Database (CMDB)

ECP 1.0 requires a simple administrative interface for the Configuration Management Database (CMDB). Verifiers on the PDP receive the endpoint data via IF-M messages sent from corresponding collectors on an endpoint and store this information in the CMDB linked to the identity of the machine where the collectors are located.

The administrative interface SHOULD enable an administrator to:

1. Query which endpoints have reported SWID tags for a particular application
2. Query which SWID tags are installed on a particular endpoint
3. Query tags based on characteristics, such as vendor, publisher, etc.

In the future, TNC intends to develop an interface to the CMDB server, which will include requirements for:

1. Creating a secure channel between a publisher and the CMDB
2. Creating a secure channel between a subscriber and the CMDB
3. The types of interactions that must be supported between publishers and subscribers to a CMDB

4.5 Network Access Requestor (NAR) and Network Access Authority (NAA)

The IF-T protocol provides a transport service for carrying the IF-TNCCS protocol messages between the endpoint and the PDP.

The NAR and NAA MUST implement IF-T TLS, since a connection is needed that:

- Can handle large volumes of data, which might require multiple roundtrips, to be sent while the device is connected
- Allows either the TNC client or TNC server to initiate a connection
- Supports secure transport based on machine certificates at both ends of the connection

The NAR and NAA MUST support the use of machine certificates for TLS at each endpoint consistent with the requirements stipulated in [IF-T TLS] and [PDP Discovery].

The NAR MUST be able to locate an authorized PDP, and switch to a new PDP when required by the network, in conformance with [PDP Discovery].

4.6 Administrative Interface and API

An interface is necessary to allow network administrators to manage the devices and software used in the Endpoint Compliance Profile. This interface SHOULD be accessible either on or through (as in the case of a remotely hosted interface) the PDP. Using this interface, an authorized user or administrator SHOULD be able to:

- Query the CMDB
- Send commands to the Verifiers, requesting information from the associated Collectors residing on network endpoints
- Update the network policy that resides on the PDP

An API is necessary to allow infrastructure devices and software access to the information stored in the CMDB. Using this API, an authorized device SHOULD be able to:

- Query the CMDB

5 Security Considerations

The Endpoint Compliance Profile offers substantial improvements in endpoint security, as evidenced by the Australian Defense Signals Directorate's analysis that 85% of targeted cyber intrusions can be prevented through application white listing, patching applications and operating systems, and using the latest versions of applications. [DSD] Despite these gains, some security risks continue to exist and must be considered.

To ensure that these benefits and risks are properly understood, this Security Considerations section includes an analysis of the benefits provided by the Endpoint Compliance Profile (section 5.1), the attacks that may be mounted against systems that implement the Endpoint Compliance Profile (section 5.2), and the countermeasures that may be used to prevent or mitigate these attacks (section □). Overall, a substantial reduction in cyber risk can be achieved.

5.1 Security Benefits of Endpoint Compliance Profile

Security weaknesses of the components for this profile for assessment and remediation should be considered in light of the practical considerations that must be addressed to have a viable solution.

Compliance has two components: assessment and remediation. The point of compliance is to ensure that authorized users are using authorized software configured to be as resilient as possible against an attack.

Compliance answers the question whether the endpoint is healthy. Our goal for compliance is to make it harder for an adversary to execute code on one of our endpoints. This profile represents an important first step in reaching that goal. If we keep our systems healthier, we are able to prevent more attacks on our endpoints and thus on our information systems.

The goal of ECP is to address compliance in stages. Stage 1 is the ability to ascertain whether all devices are authorized and whether all applications are authorized and up to date. Stage 2 will attempt to address the harder problem of whether all software is configured safely. Eventually, the goal is to also address remediation; that presents a far greater security challenge than reporting, since remediation implies the ability of a remote party to modify software or its settings on endpoints.

A second security consideration is how to gain visibility over every type of endpoint and every piece of software installed on the endpoint. This is a problem of scaling and observation. A solution is needed that can report from every type of endpoint. All software on the endpoint has to be discovered. Information about the software has to be up to date and accurate. The information that is discovered has to be reported in a consistent format, so administrators do not have to squander time deciphering proprietary systems and the information can be made readily useful for other security automation purposes.

ECP is based on a model of a standards-based schema, a standards-based set of protocols and interfaces, and the existence of an oversight group, the TCG, that can perform compliance and compatibility testing of all the components of the solution.

The data elements in the schema determine what work can be done consistently for every endpoint and every piece of software. How the data gets populated is an important consideration. ECP leverages the SWID tags from ISO 19770-2 because the tag originates with a single authoritative source, the application vendor itself. Moreover, there is a natural incentive for the vendor to create this content, since it makes it easier for enterprises and vendors to track whether software is licensed. Practical considerations are security considerations. A sustainable business model for obtaining all the necessary content is a fundamental requirement.

The TNC model is based on having a client run on an endpoint that reports to a server. The advantages are easy to list. A platform vendor can implement its own client and have it be compatible with the TNC server from a different vendor. The interfaces are layered on top of mature protocols such as TLS. TLS is the protocol of choice for ECP, since:

- it has proven secure properties,

- it can be implemented on most types of endpoints,
- it allows the gathering of large amounts of information when a device is connected, and
- it enables use of a mechanism to ensure that the client is authenticated (authorized)- a client certificate- which also provides a consistent identifier.

Mature protocols that can be implemented on most types of endpoints and a standards-based schema with a sustainable business model are both critical security considerations for compliance.

Additionally, it is important to consider the future stages for ECP. Assessment will be followed by remediation. Ensuring that clients are taking instructions only from authorized parties will be critical. Inasmuch as it is practical, enterprises will want to use the same infrastructure and investment in PKI to send those instructions to a client.

Likewise, as more information with more value is gathered from endpoints, we will also want to ensure that this information is only released to authorized applications and parties. For the next stage of ECP, TCG intends to define an interface on the CMDB that can be queried by other security automation applications to make it easier to detect attacks and for other security automation applications. This interface has to be standards-based for enterprises to reap the benefits of innovation that can be achieved by making the enterprise's data available to other tools and services.

Finally, there is compliance testing. What differentiates TCG from an IETF or ISO is the ability to ensure that products from different vendors running on different platforms will work together. We need testing to ensure that clients and collectors on various platforms will be interoperable and compatible with TNC servers and the CMDB. If pieces don't fit and work together, we cannot take advantage of the benefits of the ECP. That's a security consideration, too.

5.2 Threat Model

This section lists the attacks that can be mounted on an Endpoint Compliance Profile environment. The following section (□) describes countermeasures.

Because the Endpoint Compliance Profile describes a specific use case for TNC components, many security considerations for these components are addressed in more detail in the technical specifications: [SWID Messages for IF-M], [IF-IMC], [IF-TNCCS], [PDP Discovery], [IF-T TLS], [IF-T Tunneled EAP], [IF-PEP], [IF-IMV].

5.2.1 Endpoint Attacks

While the Endpoint Compliance Profile provides substantial improvements in endpoint security as described in section 5.1, a certain percentage of endpoints will always get compromised. For this reason, all parties must regard data coming from endpoints as potentially unreliable or even malicious. An analogy can be drawn with human testimony in an investigation or trial. Human testimony is essential but must be regarded with suspicion.

- Compromise of Endpoint

  A compromised endpoint may report false information to confuse or even provide maliciously crafted information with a goal of infecting others.

- Putting Bad Information in SWID Repository

  Even if an endpoint is not completely compromised, some of the software running on it may be unreliable or even malicious. This software, potentially including the SWID generation or discovery tool, or malicious software pretending to be a SWID generation or discovery tool, can place incorrect or maliciously crafted information into the SWID repository. Endpoint users may even place such information in the repository, whether motivated by curiosity or confusion or a desire to bypass restrictions on their use of the endpoint.

- Identity Spoofing (Impersonation)

A compromised endpoint may attempt to impersonate another endpoint to gain its privileges or to besmirch the reputation of that other endpoint.

5.2.2 Network Attacks

A variety of attacks can be mounted using the network. Generally, the network cannot be trusted.

- Eavesdropping, Modification, Injection, Replay, Deletion
- Traffic Analysis
- Denial of Service & Blocking Traffic

5.2.3 PDP Attacks

The PDP is a critical security element and therefore merits considerable scrutiny.

- Compromised Trusted PDP

  A compromised PDP or a malicious party that is able to impersonate a PDP can incorrectly grant or deny access to endpoints, place incorrect information into the CMDB, or send malicious messages such as remediation instructions to endpoints.

- Misconfiguration of Trusted PDP

  Accidental or purposeful misconfiguration of a trusted PDP can cause effects that are similar to those listed for Compromised Trusted PDP.

- Malicious Untrusted PDP

  An untrusted PDP cannot mount any significant attacks because all properly implemented endpoints and PEPs will refuse to engage in any meaningful dialog with such a PDP.

5.2.4 CMDB Attacks

The CMDB is also an important security element and therefore merits careful scrutiny.

- Putting Bad Information into Trusted CMDB

  An authorized CMDB client such as a PDP may be able to put incorrect information into a trusted CMDB or delete or modify historical information, causing incorrect decisions about endpoint security. Placing maliciously crafted data in the CMDB could even lead to compromise of CMDB clients, if they fail to carefully check such data.

- Compromised Trusted CMDB

  A compromised trusted CMDB or a malicious untrusted CMDB that is able to impersonate a trusted CMDB can lead to effects similar to those listed for “Putting Bad Information into Trusted CMDB”. Further, a compromised trusted CMDB can report different results to different CMDB clients or deny access to the CMDB for selected CMDB clients.

- Misconfiguration of Trusted CMDB

  Accidental or purposeful misconfiguration of a trusted CMDB can deny access to the CMDB or result in loss of historical data.

- Malicious Untrusted CMDB

  An untrusted CMDB cannot mount any significant attacks because all properly implemented CMDB clients will refuse to engage in any meaningful dialog with such a CMDB.

5.3 Countermeasures

This section lists the countermeasures that can be used in an Endpoint Compliance Profile environment.

5.3.1 Countermeasures for Endpoint Attacks

This profile is in and of itself a countermeasure for a compromised endpoint. A primary defense for an endpoint is to run up to date software configured to be run as safely as possible.

Ensuring that anti-virus signatures are up to date and that a firewall is configured are also protections for an endpoint that are supported by the current TNC specifications.

Endpoints that have TPMs that are provisioned by the enterprise can protect the private keys used for authentication and help prevent adversaries from stealing credentials that can be used for impersonation. Future versions of the Endpoint Compliance Profile will discuss in greater detail how to use a TPM to protect credentials and to protect the integrity of the code that executes during the bootstrap process.

5.3.2 Countermeasures for Network Attacks

To address network attacks, the IF-T for Tunneled EAP Methods and IF-T for TLS specifications both include required encryption, authentication, integrity protection, and replay protection. The PDP Discovery and Validation specification also includes authorization checks to ensure that only authorized PDPs are trusted by endpoints. Any unspecified or not yet specified network protocols employed in the Endpoint Compliance Profile (e.g. the protocol used to interface with the CMDB) should include similar protections.

These protections reduce the scope of the network threat to traffic analysis and denial of service. Countermeasures for traffic analysis (e.g. masking) are usually impractical but may be employed. Countermeasures for denial of service (e.g. detecting and blocking particular sources) SHOULD be used when appropriate to detect and block denial of service attacks. These are routine practices in network security.

5.3.3 Countermeasures for PDP Attacks

Because of the serious consequences of PDP compromise, PDPs SHOULD be especially well hardened against attack and minimized to reduce their attack surface. They SHOULD be monitored using the TNC protocols to ensure the integrity of the MAP Server and SHOULD utilize a Trusted Platform Module (TPM) for identity and/or integrity measurements of the PDP. They should be well managed to minimize vulnerabilities in the underlying platform and in systems upon which the PDP depends. Network security measures such as firewalls or intrusion detection systems may be used to monitor and limit traffic to and from the PDP. Personnel with administrative access to the PDP should be carefully screened and monitored to detect problems as soon as possible. PDP administrators should not use password-based authentication but should instead use non-reusable credentials and multi-factor authentication (where available). Physical security measures should be employed to prevent physical attacks on PDPs.

To ease detection of PDP compromise should it occur, PDP behavior should be monitored to detect unusual behavior (such as a PDP reboot, unusual traffic patterns, or other odd behavior). Endpoints should log and/or notify users and/or administrators when peculiar PDP behavior is detected. To aid forensic investigation, permanent read-only audit logs of security-relevant information pertaining to PDPs (especially administrative actions) should be maintained. If PDP compromise is detected, the PDP's certificate should be revoked and careful analysis should be performed of the source and impact of this compromise. Any reusable credentials that may have been compromised should be reissued.

Endpoints can reduce the threat of PDP compromise by minimizing the number of trusted PDPs, using the mechanisms described in the PDP Discovery and Validation specification.

5.3.4 Countermeasures for CMDB Attacks

If the host for the CMDB is located on its own device, it should be protected with the same measures taken to protect the PDP. In this circumstance, all messages between the PDP and CMDB should be protected with a mature security protocol such as TLS or IPsec.

The CMDB can aid in the detection of compromised endpoints if an adversary cannot tamper with its contents. For instance, if an endpoint reports that it does not have an application with a known vulnerability installed, an administrator can check whether the endpoint might be lying by querying the CMDB for the history of what applications were installed on the endpoint.

To help prevent tampering with the information in the database:

1. Only authorized parties should have privilege to run code on the device and to change the CMDB.
2. If a separate device hosts the CMDB, then the functionality of that device should be limited to hosting the CMDB. The firewall on the CMDB should only allow access to the PDP and to any device authorized for administration.
3. The CMDB should ideally use “write once” media to archive the history of what was placed in the CMDB, to include a snapshot of the current status of applications on endpoints.

6 Privacy Considerations

The Endpoint Compliance Profile specifically addresses the collection of compliance data from enterprise devices by an enterprise network. As such, privacy is not going to often arise as a concern for those deploying this solution.

A possible exception may be the concerns a user may have when attempting to connect a personal device (such as a phone or mobile device) to an enterprise network. The user may not want to share certain details, such as a device identifier or SWID tags, with the enterprise. The user can configure their TNCC to reject requests for this information; however, it is possible that the enterprise network policy will not allow the user's device to connect to the network without providing the requested data.

7 Endpoint Compliance Profile Examples

7.1 Continuous Monitoring of an Endpoint

An endpoint is continuously connected to a compliance-dedicated PDP using IF-T TLS.

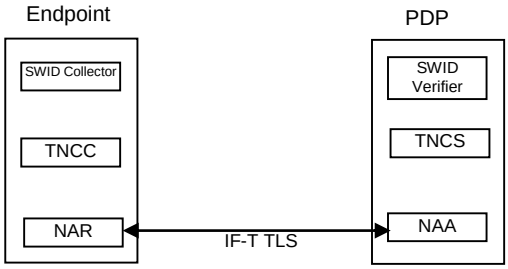


Figure 4: Continuous Monitoring of an Endpoint

7.1.1 Change on Endpoint Triggers Compliance Report

A new application is installed on the endpoint, and the SWID directory is updated. This triggers an update from the SWID Collector to the SWID Verifier. The message is sent down the TNC stack, encapsulated by TNC protocols until it is sent by the NAR to the NAA. The NAA then forwards it up through the stack, where the layers of encapsulation are removed until the SWID Message arrives at the SWID Verifier.

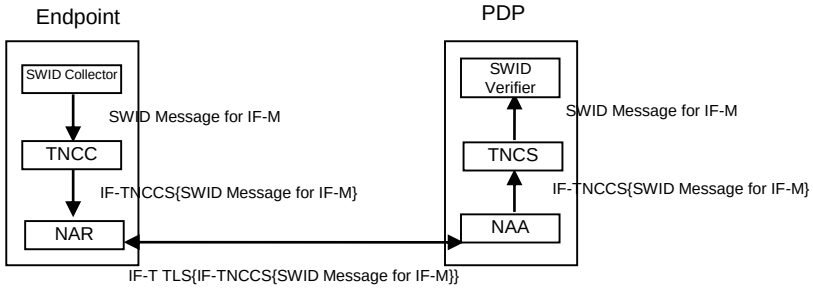


Figure 5: Compliance Protocol Encapsulation

The SWID Verifier stores the new tag information in the CMDB. If the tag indicates that the endpoint is compliant to network policy, then the process is complete until the next time an update is needed (either because policy states that the endpoint must submit a report periodically or because an install/uninstall/update on the endpoint triggers a report).

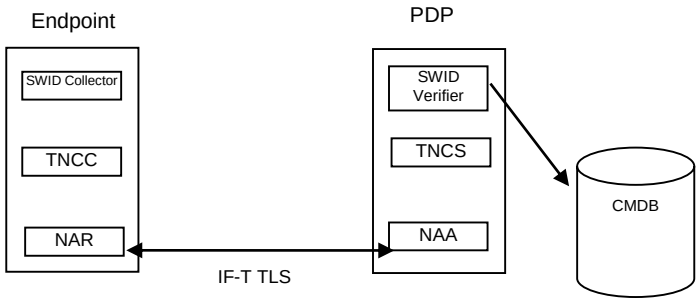


Figure 6: Storing SWIDs in the CMDB

If the endpoint has fallen out of compliance with network policy, the PDP can alert the network administrator via the PDP's administrative interface. The administrator can then take steps to remediate the problem. If the administrator has already established a policy for automatically remediating this problem, that policy will be followed.

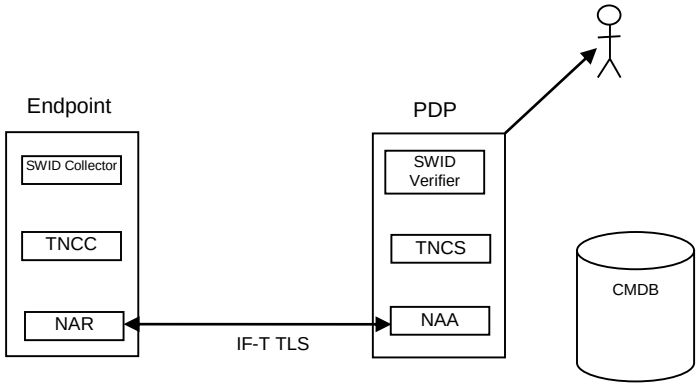


Figure 6: PDP Alerts Network Admin

7.2 Network Administrator Searches for Vulnerable Endpoints

An announcement is made that a particular version of a piece of software has a vulnerability. The network administrator uses the Administrative Interface on the PDP to search the CMDB for endpoints that reported the SWID tag for the vulnerable software.

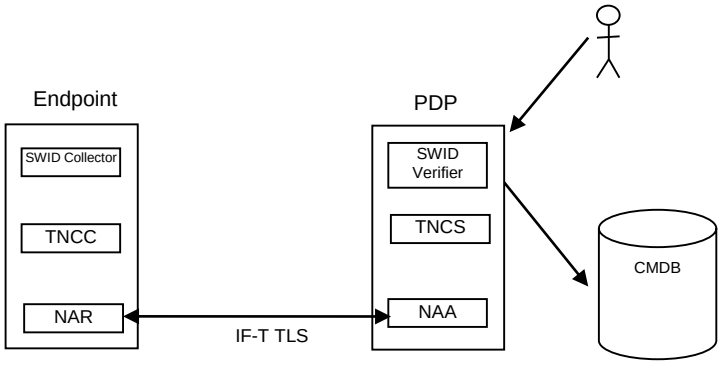


Figure 7: Admin Searches for Vulnerable Endpoints

The CMDB returns a list of entries in the database matching the administrator's search. The administrator can then remediate the vulnerable endpoints by removing it from the network, quarantining it, or updating the vulnerable software.

8 Appendix A: Comply to Connect

The Endpoint Compliance Profile levies requirements on software and infrastructure participating in compliance checking of network connected endpoints. It is assumed throughout the profile that the endpoints sending SWID messages over IF-M are already connected to the network and have been issued IP addresses. In certain circumstances, however, an enterprise may wish to perform a brief compliance check prior to allowing an endpoint to join the network. Implementing a network access control solution provides several benefits, including:

- greater assurance that the endpoint is compliant to network policy before it gains access to network resources; and
- the ability, using TNC standards, to quarantine or remove an endpoint from the network if it falls out of compliance to policy while it is connected.

While nothing in the Endpoint Compliance Profile requires the implementation of a comply-to-connect solution, the below use case and requirements are included for those implementers who wish to offer both comply-to-connect and connected-and-compliant services.

8.1 Comply-to-Connect Use Case

An endpoint seeks access to the network by completing a brief compliance check over TNC protocols before being assigned an IP address. Performing this check prior to network connection allows for efficient quarantine or removal, via standardized protocols, of endpoints that fall out of compliance or that fail the connected-and-compliant check described above.

1) The endpoint locates and validates a Policy Decision Point (PDP) in compliance with [PDP Discovery and Validation];

2) Either the TNCC on the endpoint or the TNCS on the PDP initiates a brief IF-M compliance check when the endpoint first attempts to connect to the network. These checks may include exchanging information about the state of the endpoint's firewall, etc. This report is generated by the endpoint's IMCs, and is sent from the NAR to the NAA via IF-T for Tunneled EAP.

3) The Verifiers parse the results of this check, and make a recommendation to the TNCS about whether or not to allow the device to join the network. The TNCS compiles recommendations from the Verifiers and makes a connectivity decision about the endpoint based on network policy.

a) If the endpoint is found to be out of compliance with network policy for newly-connecting devices, it may, for example, be sent to a remediation VLAN, sent to quarantine, or blocked from the network via IF-PEP.

b) If the endpoint meets network policy for newly connecting devices, it is assigned an IP address and allowed on the network.

4) Because the device used IF-T for Tunneled EAP for its initial connection to the PDP, it can now be quarantined or removed from the network if it ever fails the connected-and-compliant health check. Using IF-PEP, the TNCS can move the endpoint to a remediation or quarantine VLAN, or remove its ability to access the network entirely, if it is found to be out of compliance with network policy.

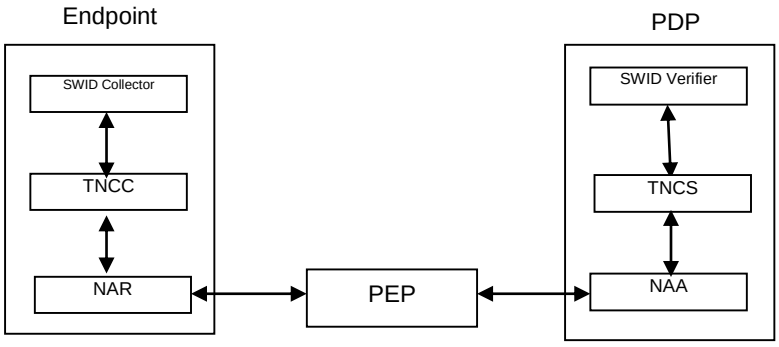


Figure 8: Comply-to-Connect Use Case

8.2 Comply-to-Connect Requirements

8.2.1 IF-M Collectors and Verifiers

Section 4.2 of the Endpoint Compliance Profile already requires that any verifier used as part of this solution must be compliant with [IF-IMV], and any collector used as part of this solution must be compliant with [IF-IMC]. This requirement is therefore true of any collectors and verifiers used to provide additional comply-to-connect capabilities as a part of the connected-and-compliant solution offered within this profile.

An enterprise may choose to perform any sort of compliance check prior to granting an endpoint access to the network; these checks SHOULD be performed using the [IF-M] schema.

8.2.2 The Network Access Requestor (NAR) and Network Access Authority (NAA)

For conformance to the Endpoint Compliance Profile, the NAR and NAA must be able to communicate via IF-T TLS. For additional comply-to-connect capabilities, the NAR and NAA SHOULD be conformant to [IF-T Tunneled EAP].

8.2.3 Policy Enforcement Point (PEP)

The enterprise might decide to restrict access to an endpoint that has an application with a version that needs to be upgraded or patched. If the endpoint is connected to a policy enforcement point (PEP) that is controlled by a RADIUS-based PDP, then an enforcement message can be sent to the PEP to isolate the endpoint.

Any PEP used in accordance with this profile MUST be conformant with [IF-PEP].

8.2.4 Administrative Interface

For solutions that include a PEP, the Administrative Interface SHOULD enable an administrator to send commands to the PEP to either quarantine or remove an endpoint from the network.

9 References

9.1 Normative References

[IF-IMC] Trusted Computing Group, *TNC IF-IMC*, Specification Version 1.3, February 2013

[IF-IMV] Trusted Computing Group, *TNC IF-IMV*, Specification Version 1.4, December 2014

[IF-T Tunneled EAP] Trusted Computing Group, *TNC IF-T: Protocol Bindings for Tunneled EAP Methods*, Specification Version 1.1, Revision 10, May 2007

[IF-T TLS] Trusted Computing Group, *TNC IF-T: Binding to TLS*, Specification Version 2.0, Revision 7, February 2013

[IF-TNCCS] Trusted Computing Group, *TNC IF-TNCCS: TLV Binding*, Specification Version 2.0, Revision 16, January 2010

[IF-PEP] Trusted Computing Group, *TNC IF-PEP: Protocol Bindings for RADIUS*, Specification Version 1.1, February 2007

[PDP Discovery] Trusted Computing Group, *PDP Discovery and Validation*, Specification Version 1.0, PUBLIC REVIEW

[RFC 2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", Internet Engineering Task Force RFC 2119, March 1997.

[SWID] ISO/IEC 19770-2:2009, *Information technology—Software asset management—Part 2: Software identification tag.*

[SWID Messages for IF-M] Trusted Computing Group, *SWID Messages for IF-M*, Specification Version 1.0, PUBLIC REVIEW

[TNC Architecture] Trusted Computing Group, *TNC Architecture for Interoperability*, Specification Version 1.5, Revision 3, May 20012.

9.2 Informative References

[IEEE 802.1ar] Boraz, Mike and Max Pritikin. "Secure Device Identity". IEEE 802.1ar. December 2009.

[RFC 5209] Sangster, P. et al., "Network Endpoint Assessment (NEA): Overview and Requirements", Internet Engineering Task Force RFC 5209, June 2008.

[DSD] http://www.dsd.gov.au/publications/csocprotect/top_4_mitigations.htm

[SANS] **http://www.sans.org/critical-security-controls/**