TCG Trusted Network Connect Compliance_TNC Interoperability Test Plan

Version 1.1
Revision 6
26 September 2011
Published

Contact:
admin@trustedcomputinggroup.org

TCG

TCG PUBLISHED

Disclaimer

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

Acknowledgement

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

Special thanks to the following individuals who contributed to this document:

Sung Lee	
Mauricio Sanchez	
Brad Upson	
Steve Hanna	

Table of Contents

1 Introduction

This section summarizes the purpose and intended audience for this document.

1.1 Purpose

The purpose of this document is to define test cases that determine whether multiple implementations of the TNC IF-PEP for RADIUS [1], TNC IF-IMC [2], TNC IF-IMV [3] TNC IF-TNCCS [6], TNC IF-TNCCS-SOH [7], TNC IF-MAP [8][9], and TNC IF-MAP Metadata for Network Security [10] specifications, or multiple versions of a single implementation of those specifications, can interoperate with each other. In particular, it defines and lists all the use cases that must be passed to prove interoperability in accordance with the listed TCG specifications. This document does not contain any normative statements.

1.2 Intended Audience

The intended audience for this document includes test designers and implementers, as well as product developers and customers who need to understand the TNC specification interoperability tests. Readers should be familiar with the Compliance_TNC Compliance and Interoperability Principles specification [4], the TNC Architecture [5], and with the interface specifications listed in section 1.1.

2 Specifications and Components

2.1 Specifications

This document is based on the TNC IF-PEP for RADIUS v1.0 specification [1], the TNC IF-IMC v1.1 specification [2], the TNC IF-IMV v1.1 specification [3], the TNC IF-TNCCS v1.1 specification [6], the TNC IF-TNCCS: Protocol Bindings for SoH v1.0 specification [7], the TNC IF-MAP Bindings for SOAP v2.0 specification [8], and the Compliance_TNC Compliance and Interoperability Principles document [4]. The IF-PEP for RADIUS v1.0 specification defines the IF-PEP interface. The IF-IMC v1.1 specification defines the IF-IMC interface. The IF-IMV v1.1 specification defines the IF-IMV interface. The IF-TNCCS v1.1 specification defines the IF-TNCCS interface. The TNC IF-TNCCS: Protocol Bindings for SoH v1.0 specification defines the IF-TNCCS-SOH interface. The TNC IF-MAP Bindings for SOAP v1.1 and 2.0 specifications define the IF-MAP interface. The TNC IF-MAP Metadata for Network Security 1.0 specification defines network security metadata. The Compliance_TNC Compliance and Interoperability Principles document provides an overview of the Compliance_TNC testing.

2.2 Components

The components to be tested provide functions of the roles defined in the TNC Architecture specification [5]. The roles and functions are listed here; components to be tested are in bold. For definitions of and more information about these components, see the TNC Architecture specification.

2.2.1 Access Requestor

The Access Requestor (AR) consists of the following functions:

- *Network Access Requestor (NAR)*
- ***TNC Client (TNCC)***
- ***Integrity Measurement Collector (IMC)***

2.2.2 Policy Enforcement Point

The Policy Enforcement Point (PEP) consists of the following functions:

- ***Network Access Enforcer (NAE)***

2.2.3 Policy Decision Point

The Policy Decision Point (PDP) consists of the following functions:

- *Network Access Authority (NAA)*
- ***TNC Server (TNCS)***
- ***Integrity Measurement Verifier (IMV)***

2.2.4 Metadata Access Point

The Metadata Access Point Server (MAP) consists of the following functions:

- ***Metadata Access Point Server (MAPS)***

2.2.5 Metadata Access Point Client

Examples of Metadata Access Point Clients (MAPCs) include:

- *PDPs*

- ***Flow Controllers***
- ***Sensors***
- ***Other MAP Clients such as data visualizers***

3 Interoperability Scenarios

This section lists specific interoperability scenarios to be tested in order to meet the interoperability goals and/or requirements defined in the referenced TCG specifications or in the Compliance and Interoperability Principles. A separate subsection is provided for each interoperability scenario so the scenario can be described in detail.

Each interoperability scenario description includes preconditions, the components involved, the interfaces by which these components interact, and specific test steps. It describes the expected outcome and how this outcome can be measured. It also describes any expected or anticipated failures and how they can be detected.

All interoperability scenarios are required unless specific exceptions are defined within the scenario.

3.1 Test IMC and IMV with TNCC and TNCS via IF-IMC and IF-IMV

All of the interoperability test cases in this section share the following basic test parameters. Other test parameters vary from one test case to the next so they are called out separately.

Components involved:

- IMC, IMV, TNCC, and TNCS. Other components may also be present.

Interfaces by which these components interact:

- IF-IMC and IF-IMV

Specifications that define these interfaces:

- IF-IMC 1.1 [2] and IF-IMV 1.1 [3]

3.1.1 Simple Allow

Preconditions:

- An IMC is installed on an AR with a TNCC. An IMV is installed on a PDP with a TNCS.
    - This test focuses on interoperability between the IMC and TNCC across IF-IMC and between the IMV and TNCS across IF-IMV, so the IMC and IMV should be known or expected to interoperate with each other and the TNCC and TNCS should similarly be known or expected to function properly together.
- The TNCS should be configured so that an Allow recommendation from the IMV will cause the TNCS-Recommendation to be Allow and another recommendation from the IMV will cause the TNCS-Recommendation to be Deny.
- A NAR, NAA, and NAE will generally be used in this test also but they are not the components under test.
    - If used, the NAR, NAA, and NAE should be configured so that an Allow recommendation from the TNCS will permit network access and another recommendation from the TNCS will block or restrict network access.

Test Steps:

- The AR, IMC, and IMV are configured so that the IMV will provide an Allow recommendation.
- The AR is connected to the network or other steps are taken to cause the TNCC and TNCS to begin an Integrity Check Handshake.

Expected Outcome:

- The TNCC and TNCS should complete the Integrity Check Handshake, the IMV should provide an Allow recommendation, and the TNCS should also provide an Allow recommendation.
    - Measurement of this outcome can be implementation-specific.
- If an NAA and NAE are used, this should cause the NAA and NAE to permit network access.
    - This outcome can be measured by attempting to access the network from the AR after the Integrity Check Handshake has completed. Network access should be successful.

Anticipated Failures:

- If network access from the AR is unsuccessful or isolated after the Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the IMC, IMV, TNCC, or TNCS has malfunctioned.
    - To diagnose the problem, logs may be used to determine what messages were sent between the IMC and IMV and what recommendations the IMV and TNCS provided.

3.1.2 Simple Deny

Preconditions:

- An IMC is installed on an AR with a TNCC. An IMV is installed on a PDP with a TNCS.
    - This test focuses on interoperability between the IMC and TNCC across IF-IMC and between the IMV and TNCS across IF-IMV, so the IMC and IMV should be known or expected to interoperate with each other and the TNCC and TNCS should similarly be known or expected to function properly together.
- The TNCS should be configured so that a Deny recommendation from the IMV will cause the TNCS-Recommendation to be Deny and another recommendation from the IMV will cause the TNCS-Recommendation to be Allow.
- A NAR, NAA, and NAE will generally be used in this test also but they are not the components under test.
    - If used, the NAR, NAA, and NAE should be configured so that a Deny recommendation from the TNCS will block or restrict network access and another recommendation from the TNCS will permit network access.

Test Steps:

- The AR, IMC, and IMV are configured so that the IMV will provide a Deny recommendation.
- The AR is connected to the network or other steps are taken to cause the TNCC and TNCS to begin an Integrity Check Handshake.

Expected Outcome:

- The TNCC and TNCS should complete the Integrity Check Handshake, the IMV should provide a Deny recommendation, and the TNCS should also provide a Deny recommendation.
    - Measurement of this outcome can be implementation-specific.
- If an NAA and NAE are used, this should cause the NAA and NAE to block or restrict network access.

  - This outcome can be measured by attempting to access the network from the AR after the Integrity Check Handshake has completed. Network access should be unsuccessful or isolated.

Anticipated Failures:

- If network access from the AR is successful after the Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the IMC, IMV, TNCC, or TNCS has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the IMC and IMV and what recommendations the IMV and TNCS provided.

3.1.3 Deny with Remediation

This test case is required only for IMC/IMV and TNCC/TNCS implementations that support the ability to dynamically reassess compliance.

Preconditions:

- An IMC is installed on an AR with a TNCC. An IMV is installed on a PDP with a TNCS.
  - This test focuses on interoperability between the IMC and TNCC across IF-IMC and between the IMV and TNCS across IF-IMV, so the IMC and IMV should be known or expected to interoperate with each other and the TNCC and TNCS should similarly be known or expected to function properly together.
- The TNCS should be configured so that a Deny recommendation from the IMV will cause the TNCS-Recommendation to be Deny and an Allow recommendation from the IMV will cause the TNCS-Recommendation to be Allow.
- The AR should be configured so that the IMV provides a Deny recommendation initially and an Allow recommendation after remediation.
- A NAR, NAA, and NAE will generally be used in this test also but they are not the components under test.
  - If used, the NAR, NAA, and NAE should be configured so that a Deny recommendation from the TNCS will block or restrict network access and an Allow recommendation from the TNCS will permit network access.

Test Steps:

- The AR, IMC, and IMV are configured so that the IMV will provide a Deny recommendation.
- The AR is connected to the network or other steps are taken to cause the TNCC and TNCS to begin an Integrity Check Handshake.
- After the Integrity Check Handshake is completed (Deny recommendation provided, network access blocked or isolated), remediation takes place on the AR either automatically or manually.
- The AR, IMC, and IMV are now configured so that the IMV will provide an Allow recommendation, and another Integrity Check Handshake is requested.

Expected Outcome:

- The TNCC and TNCS should complete the initial Integrity Check Handshake, the IMV should provide a Deny recommendation, and the TNCS should also provide a Deny recommendation.
  - Measurement of this outcome can be implementation-specific.

- If an NAA and NAE are used, this should cause the NAA and NAE to block or restrict network access.
  - This outcome can be measured by attempting to access the network from the Access Requester after the Integrity Check Handshake has completed. Network access should be unsuccessful or isolated.
- Once this outcome has been verified and remediation completed, the TNCC and TNCS should complete a second Integrity Check Handshake, the IMV should provide an Allow recommendation, and the TNCS should also provide an Allow recommendation.
  - Measurement of this outcome can be implementation-specific.
- If an NAA and NAE are used, this should cause the NAA and NAE to permit network access.
  - This outcome can be measured by attempting to access the network from the Access Requester after the subsequent Integrity Check Handshake has completed. Network access should be successful.

Anticipated Failures:

- If network access from the AR is successful after the initial Integrity Check Handshake has completed, or if network access from the AR is unsuccessful or isolated after the subsequent Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the IMC, IMV, TNCC, or TNCS has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the IMC and IMV and what recommendations the IMV and TNCS provided.

3.1.4 Fault Detection

This test case is required only for IMC/IMV and TNCC/TNCS implementations that support the ability to dynamically reassess compliance

Preconditions:

- An IMC is installed on an AR with a TNCC. An IMV is installed on a PDP with a TNCS.
  - This test focuses on interoperability between the IMC and TNCC across IF-IMC and between the IMV and TNCS across IF-IMV, so the IMC and IMV should be known or expected to interoperate with each other and the TNCC and TNCS should similarly be known or expected to function properly together.
- The TNCS should be configured so that a Deny recommendation from the IMV will cause the TNCS-Recommendation to be Deny and an Allow recommendation from the IMV will cause the TNCS-Recommendation to be Allow.
- The AR should be configured so that the IMV provides an Allow recommendation initially and a Deny recommendation after a fault is introduced.
- A NAR, NAA, and NAE will generally be used in this test also but they are not the components under test.
  - If used, the NAR, NAA, and NAE should be configured so that a Deny recommendation from the TNCS will block or restrict network access and an Allow recommendation from the TNCS will permit network access.

Test Steps:

- The AR, IMC, and IMV are configured so that the IMV will provide an Allow recommendation.

- The AR is connected to the network or other steps are taken to cause the TNCC and TNCS to begin an Integrity Check Handshake.
- After the Integrity Check Handshake is completed (Allow recommendation provided, network access permitted), a fault is introduced on the AR.
- The AR, IMC, and IMV are now configured so that the IMV will provide a Deny recommendation, and another Integrity Check Handshake is requested.

Expected Outcome:

- The TNCC and TNCS should complete the initial Integrity Check Handshake, the IMV should provide an Allow recommendation, and the TNCS should also provide an Allow recommendation.
    - Measurement of this outcome can be implementation-specific.
- If an NAA and NAE are used, this should cause the NAA and NAE to permit network access.
    - This outcome can be measured by attempting to access the network from the AR after the Integrity Check Handshake has completed. Network access should be successful.
- Once this outcome has been verified and the fault is introduced, the TNCC and TNCS should complete a second Integrity Check Handshake, the IMV should provide a Deny recommendation, and the TNCS should also provide a Deny recommendation.
    - Measurement of this outcome can be implementation-specific.
- If an NAA and NAE are used, this should cause the NAA and NAE to block or restrict network access.
    - This outcome can be measured by attempting to access the network from the AR after the subsequent Integrity Check Handshake has completed. Network access should be unsuccessful or isolated.

Anticipated Failures:

- If network access from the Access Requester is unsuccessful or isolated after the initial Integrity Check Handshake has completed, or if network access from the Access Requester is successful after the second Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the IMC, IMV, TNCC, or TNCS has malfunctioned.
    - To diagnose the problem, logs may be used to determine what messages were sent between the IMC and IMV and what recommendations the IMV and TNCS provided.

3.1.5 Allow In Spite of Deny Recommendation

This test case is required only for TNCS implementations that support the ability to provide a TNCS-Recommendation different from the IMV recommendation.

Preconditions:

- An IMC is installed on an Access Requester (AR) with a TNCC. An IMV is installed on a Policy Decision Point (PDP) with a TNCS.
    - This test focuses on interoperability between the IMC and TNCC across IF-IMC and between the IMV and TNCS across IF-IMV, so the IMC and IMV should be known or expected to interoperate with each other and the TNCC and TNCS should similarly be known or expected to function properly together.

- The TNCS should be configured so that even if there is a Deny recommendation from the IMV, the TNCS-Recommendation will be Allow.
- A NAR, NAA, and NAE will generally be used in this test also but they are not the components under test.
  - If used, the NAR, NAA, and NAE should be configured so that an Allow recommendation from the TNCS will permit network access and another recommendation from the TNCS will block or restrict network access.

Test Steps:

- The AR, IMC, and IMV are configured so that the IMV will provide an Deny recommendation.
- The AR is connected to the network or other steps are taken to cause the TNCC and TNCS to begin an Integrity Check Handshake.

Expected Outcome:

- The TNCC and TNCS should complete the Integrity Check Handshake, the IMV should provide a Deny recommendation, and the TNCS should provide an Allow recommendation.
  - Measurement of this outcome can be implementation-specific.
- If an NAA and NAE are used, this should cause the NAA and NAE to permit network access.
  - This outcome can be measured by attempting to access the network from the AR after the Integrity Check Handshake has completed. Network access should be successful.

Anticipated Failures:

- If network access from the AR is unsuccessful or isolated after the Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the IMC, IMV, TNCC, or TNCS has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the IMC and IMV and what recommendations the IMV and TNCS provided.

3.1.6 Deny In Spite of Allow Recommendation

This test case is required only for TNCS implementations that support the ability to provide a TNCS-Recommendation different from the IMV recommendation.

Preconditions:

- An IMC is installed on an Access Requester (AR) with a TNCC. An IMV is installed on a Policy Decision Point (PDP) with a TNCS.
  - This test focuses on interoperability between the IMC and TNCC across IF-IMC and between the IMV and TNCS across IF-IMV, so the IMC and IMV should be known or expected to interoperate with each other and the TNCC and TNCS should similarly be known or expected to function properly together.
- The TNCS should be configured so that even if there is an Allow recommendation from the IMV, the TNCS-Recommendation will be Deny.
- A NAR, NAA, and NAE will generally be used in this test also but they are not the components under test.

  - If used, the NAR, NAA, and NAE should be configured so that a Deny recommendation from the TNCS will block or restrict network access and another recommendation from the TNCS will permit network access.

Test Steps:

- The AR, IMC, and IMV are configured so that the IMV will provide an Allow recommendation.
- The AR is connected to the network or other steps are taken to cause the TNCC and TNCS to begin an Integrity Check Handshake.

Expected Outcome:

- The TNCC and TNCS should complete the Integrity Check Handshake, the IMV should provide an Allow recommendation, and the TNCS should provide a Deny recommendation.
  - Measurement of this outcome can be implementation-specific.
- If an NAA and NAE are used, this should cause the NAA and NAE to block or restrict network access.
  - This outcome can be measured by attempting to access the network from the AR after the Integrity Check Handshake has completed. Network access should be unsuccessful or isolated.

Anticipated Failures:

- If network access from the AR is successful after the Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the IMC, IMV, TNCC, or TNCS has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the IMC and IMV and what recommendations the IMV and TNCS provided.

3.1.7 Fault Detection with Multiple IMC/IMV Pairs

This test case is required only on platforms for which multiple IMC/IMV pairs are available. Also, this test case may also be performed as "Deny with Remediation with Multiple IMC/IMV Pairs" using the test case conditions from section 3.1.3 above.

Preconditions:

- Two or more IMCs are installed on an AR with a TNCC. The corresponding IMVs are installed on a PDP with a TNCS.
  - This test focuses on interoperability between the IMCs and TNCC across IF-IMC and between the IMVs and TNCS across IF-IMV, so the IMC/IMV pairs should be known or expected to interoperate with each other and the TNCC and TNCS should similarly be known or expected to function properly together.
  - Each individual IMC/IMV pair should already be successfully tested in test cases 3.1.1-3.1.6.
- The TNCS should be configured so that a Deny recommendation from any IMV will cause the TNCS-Recommendation to be Deny and an Allow recommendation from all IMVs will cause the TNCS-Recommendation to be Allow.
- The AR should be configured so that the IMV provides an Allow recommendation initially and one or more IMVs provide a Deny recommendation after a fault is introduced.
- A NAR, NAA, and NAE will generally be used in this test also but they are not the components under test.

  - If used, the NAR, NAA, and NAE should be configured so that a Deny recommendation from the TNCS will block or restrict network access and an Allow recommendation from the TNCS will permit network access.

Test Steps:

- The AR, IMCs, and IMVs are configured so that the IMVs will provide an Allow recommendation.
- The AR is connected to the network or other steps are taken to cause the TNCC and TNCS to begin an Integrity Check Handshake.
- After the Integrity Check Handshake is completed (Allow recommendation provided, network access permitted), a fault is introduced on the AR.
- The AR, IMC, and IMV are now configured so that an IMV will provide a Deny recommendation, and another Integrity Check Handshake is requested.

Expected Outcome:

- The TNCC and TNCS should complete the initial Integrity Check Handshake, the IMVs should provide an Allow recommendation, and the TNCS should also provide an Allow recommendation.
  - Measurement of this outcome can be implementation-specific.
- If an NAA and NAE are used, this should cause the NAA and NAE to permit network access.
  - This outcome can be measured by attempting to access the network from the AR after the Integrity Check Handshake has completed. Network access should be successful.
- Once this outcome has been verified and the fault is introduced, the TNCC and TNCS should complete a second Integrity Check Handshake, an IMV should provide a Deny recommendation, and the TNCS should also provide a Deny recommendation.
  - Measurement of this outcome can be implementation-specific.
- If an NAA and NAE are used, this should cause the NAA and NAE to block or restrict network access.
  - This outcome can be measured by attempting to access the network from the AR after the subsequent Integrity Check Handshake has completed. Network access should be unsuccessful or isolated.

Anticipated Failures:

- If network access from the Access Requester is unsuccessful or isolated after the initial Integrity Check Handshake has completed, or if network access from the Access Requester is successful after the second Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the IMCs, IMVs, TNCC, or TNCS has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the IMC/IMV pairs and what recommendations the IMVs and TNCS provided.

3.2 Test PEP and PDP via IF-PEP

All of the interoperability test cases in this section share the following basic test parameters. Other test parameters vary from one test case to the next so they are called out separately.

Components involved:

- PEP and PDP. An AR is also present but is not a component under test.

Interface by which these components interact:

- IF-PEP for RADIUS

Specification that defines this interface:

- IF-PEP for RADIUS 1.0 [1]

3.2.1 Access-Accept

Preconditions:

- The AR and PDP are configured so that the PDP will send an Access-Accept message to the PEP when the AR is evaluated.
- The PEP is configured to consult with the PDP when determining network access for the AR and to permit network access whenever an Access-Accept is received.

Test Steps:

- The AR is connected to the network or other steps are taken to cause the AR and PDP to begin an Integrity Check Handshake.

Expected Outcome:

- The AR and PDP should complete the Integrity Check Handshake, the PDP should send an Access-Accept message to the PEP via IF-PEP for RADIUS, and the PEP should permit network access.
    - This outcome can be measured by attempting to access the network from the AR after the Integrity Check Handshake has completed. Network access should be successful.

Anticipated Failures:

- If network access from the AR is unsuccessful or isolated after the Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the AR, PDP, or PEP has malfunctioned.
    - To diagnose the problem, logs and/or packet captures may be used to determine what messages were sent between the AR and PDP and what messages were sent between the PDP and PEP.

3.2.2 Access-Reject

Preconditions:

- The AR and PDP are configured so that the PDP will send an Access-Reject message to the PEP when the AR is evaluated.
- The PEP is configured to consult with the PDP when determining network access for the AR and to block or isolate network access whenever an Access-Reject is received.

Test Steps:

- The AR is connected to the network or other steps are taken to cause the AR and PDP to begin an Integrity Check Handshake.

Expected Outcome:

- The AR and PDP should complete the Integrity Check Handshake, the PDP should send an Access-Reject message to the PEP via IF-PEP for RADIUS, and the PEP should block or isolate network access.

  - This outcome can be measured by attempting to access the network from the AR after the Integrity Check Handshake has completed. Network access should be unsuccessful or isolated.

Anticipated Failures:

- If network access from the AR is successful after the Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the AR, PDP, or PEP has malfunctioned.
  - To diagnose the problem, logs and/or packet captures may be used to determine what messages were sent between the AR and PDP and what messages were sent between the PDP and PEP.

3.2.3 Access-Accept with VLAN ID

This test case is required only for PEPs that intend to support VLAN-based isolation.

Preconditions:

- The AR and PDP are configured so that the PDP will send an Access-Accept message and VLAN ID (different from the native VLAN / PVID) to the PEP when the AR is evaluated.
- The PEP is configured to have a native VLAN on the interface (wired or wireless), to consult with the PDP when determining network access for the AR, to permit network access whenever an Access-Accept is received, and to assign the VLAN ID received from the PDP.

Test Steps:

- The AR is connected to the network or other steps are taken to cause the AR and PDP to begin an Integrity Check Handshake.

Expected Outcome:

- The AR and PDP should complete the Integrity Check Handshake, the PDP should send an Access-Accept message and VLAN ID to the PEP via IF-PEP for RADIUS, and the PEP should permit network access on the specified VLAN.
  - This outcome can be measured by attempting to access the network from the AR after the Integrity Check Handshake has completed. Network access should be successful and assigned to the specified VLAN.

Anticipated Failures:

- If network access from the AR is unsuccessful, isolated, or not on the specified VLAN after the Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the AR, PDP, or PEP has malfunctioned.
  - To diagnose the problem, logs and/or packet captures may be used to determine what messages were sent between the AR and PDP and what messages were sent between the PDP and PEP.

3.2.4 Access-Accept with Filter-ID

This test case is required only for PEPs that intend to support filter-based isolation.

Preconditions:

- The AR and PDP are configured so that the PDP will send an Access-Accept message and Filter-ID to the PEP when the AR is evaluated.

- The PEP is configured to consult with the PDP when determining network access for the AR, to permit network access whenever an Access-Accept is received, and to apply the Filter-ID received from the PDP.

Test Steps:

- The AR is connected to the network or other steps are taken to cause the AR and PDP to begin an Integrity Check Handshake.

Expected Outcome:

- The AR and PDP should complete the Integrity Check Handshake, the PDP should send an Access-Accept message and Filter-ID to the PEP via IF-PEP for RADIUS, and the PEP should permit network access with the specified Filter-ID applied.
    - This outcome can be measured by attempting to access the network from the AR after the Integrity Check Handshake has completed. Network access should be successful and the specified Filter-ID should be applied.

Anticipated Failures:

- If network access from the AR is unsuccessful, isolated, or the specified Filter-ID is not applied after the Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the AR, PDP, or PEP has malfunctioned.
    - To diagnose the problem, logs and/or packet captures may be used to determine what messages were sent between the AR and PDP and what messages were sent between the PDP and PEP.

3.3 Test TNCC and TNCS via IF-TNCCS or IF-TNCCS-SOH

All of the interoperability test cases in this section share the following basic test parameters. Other test parameters vary from one test case to the next so they are called out separately.

Components involved:

- TNCC and TNCS. Other components may also be present.

Interfaces by which these components interact:

- IF-TNCCS or IF-TNCCS-SOH

Specifications that define these interfaces:

- IF-TNCCS [6] or IF-TNCCS: Protocol Bindings for SoH [7][7]

3.3.1 Simple Allow

Preconditions:

- A TNCC is installed on an AR with an IMC. A TNCS is installed on a PDP with an IMV.
    - This test focuses on interoperability between the TNCC and TNCS across IF-TNCCS-SOH, so the IMC and IMV should be known or expected to interoperate with each other.
- The TNCS should be configured so that an Allow recommendation from the IMV will cause the TNCS-Recommendation to be Allow and another recommendation from the IMV will cause the TNCS-Recommendation to be Deny.
- A NAR, NAA, and NAE will generally be used in this test also but they are not the components under test.

  - If used, the NAR, NAA, and NAE should be configured so that an Allow recommendation from the TNCS will permit network access and another recommendation from the TNCS will block or restrict network access.

Test Steps:

- The AR, TNCS, and IMV are configured so that the IMV will provide an Allow recommendation.
- The AR is connected to the network or other steps are taken to cause the TNCC and TNCS to begin an Integrity Check Handshake.

Expected Outcome:

- The TNCC and TNCS should complete the Integrity Check Handshake, the IMV should provide an Allow recommendation, and the TNCS should also provide an Allow recommendation.

  When using IF-TNCCS-SOH, this should cause the TNCS to send an SOHR with MS-Quarantine-State that indicates success (qState value of 1). When using IF-TNCCS 1.0, this should cause the TNCS to send a TNCCS-Recommendation of allow.

  - Measurement of this outcome is by observing the end state of the integrity check process in the client and server UI and/or logs. If the client or server provides an indication of success or failure, the state should be success.
- If an NAA and NAE are used, this should cause the NAA and NAE to permit network access.
  - This outcome can be measured by attempting to access the network from the AR after the Integrity Check Handshake has completed. Network access should be successful.

Anticipated Failures:

- If the end state of the integrity check process is not success, or if network access from the AR is unsuccessful or isolated, after the Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the IMC, IMV, TNCC, or TNCS has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the TNCS and TNCC and what recommendations the IMV and TNCS provided.

3.3.2 Simple Deny

Preconditions:

- A TNCC is installed on an AR with an IMC. A TNCS is installed on a PDP with an IMV.
  - This test focuses on interoperability between the TNCC and TNCS across IF-TNCCS-SOH, so the IMC and IMV should be known or expected to interoperate with each other.
- The TNCS should be configured so that a Deny recommendation from the IMV will cause the TNCS-Recommendation to be Deny and another recommendation from the IMV will cause the TNCS-Recommendation to be Allow.
- A NAR, NAA, and NAE will generally be used in this test also but they are not the components under test.
  - If used, the NAR, NAA, and NAE should be configured so that a Deny recommendation from the TNCS will block or restrict network access and another recommendation from the TNCS will permit network access.

Test Steps:

- The AR, TNCS and IMV are configured so that the IMV will provide a Deny recommendation.
- The AR is connected to the network or other steps are taken to cause the TNCC and TNCS to begin an Integrity Check Handshake.

Expected Outcome:

- The TNCC and TNCS should complete the Integrity Check Handshake, the IMV should provide a Deny recommendation, and the TNCS should also provide a Deny recommendation.

  When using IF-TNCCS-SOH, this should cause the TNCS to send an SOHR with MS-Quarantine-State that indicates success (qState value of 0). When using IF-TNCCS 1.0, this should cause the TNCS to send a TNCCS-Recommendation of deny.

  - Measurement of this outcome is by observing the end state of the integrity check process in the client and server UI and/or logs. If the client or server provides an indication of success or failure, the state should be failure.
- If an NAA and NAE are used, this should cause the NAA and NAE to block or restrict network access.
  - This outcome can be measured by attempting to access the network from the AR after the Integrity Check Handshake has completed. Network access should be unsuccessful or isolated.

Anticipated Failures:

- If network access from the AR is successful after the Integrity Check Handshake has completed, then either one of the preconditions has not been met or one or more of the IMC, IMV, TNCC, or TNCS has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the TNCS and TNCC and what recommendations the IMV and TNCS provided.

3.4 Test MAP Server and MAP Client via IF-MAP

All of the interoperability test cases in this section share the following basic test parameters. Other test parameters vary from one test case to the next so they are called out separately. To pass these tests, MAP Clients must successfully interoperate in all tests relevant to the MAP Client’s role, and MAP Servers must successfully interoperate with all MAP Clients presented for testing.

Components involved:

- MAP Server and MAP Client. Other components may also be present.
  - Specifically, an AR may be represented by an actual endpoint or test tool(s) capable of generating authentication requests, traffic, and Sensor events.
  - For the Search/Consume and Subscribe/Consume test cases, the device under test may only respond to certain metadata changes. If that’s the case (and it usually is), the Sensor or test tool must be configured to publish the kind of metadata change supported by the device under test.

Interfaces by which these components interact:

- IF-MAP

Specifications that define these interfaces:

- IF-MAP Bindings for SOAP 1.1 [8]
- IF-MAP Bindings for SOAP 2.0 [9]
- IF-MAP Metadata for Network Security 1.0 [10]

3.4.1 PDP Publish / Delete

Preconditions:

- A PDP is acting as a MAP Client. A MAP Server is installed on a MAP.
- The PDP should be configured so that when an AR successfully connects to the network, the MAP Client on the PDP publishes metadata (MAC address, IP address, VLAN, other status, and/or optional identity/integrity information) to the MAP.
- An AR and PEP will generally be used in this test also but they are not the components under test.
    - If used, the AR and PEP should be configured to allow an authenticated AR to access the network.

Test Steps:

- The AR is authenticated to the network or other steps are taken to cause the PDP to register an authenticated session.
- The AR disconnects from the network.

Expected Outcome:

- When the PDP successfully authenticates the AR, it should publish metadata (MAC address, IP address, VLAN, other status, and/or optional identity/integrity information) to the MAP.
    - Measurement of this outcome is by observing or querying the MAP database to determine that metadata for that session is present.
- When the AR disconnects from the network, the PDP should delete the metadata that it published for that session.
    - Measurement of this outcome is by observing or querying the MAP database to determine that metadata for that session is no longer present.

Anticipated Failures:

- If the appropriate metadata does not show up in the MAP after the AR successfully connects to the network, or remains in the MAP after the AR disconnects from the network, then either one of the preconditions has not been met or one or more of the PDP, MAP Client, or MAP Server has malfunctioned.
    - To diagnose the problem, logs may be used to determine what messages were sent between the MAP Client and the MAP Server.

3.4.2 PDP Search / Consume

This test case is required only for MAP Client implementations that support the ability to search for metadata and apply policy based upon search results.

Preconditions:

- A PDP is acting as a MAP Client. A MAP Server is installed on a MAP.
- The MAP database is pre-populated with metadata (such as ip-mac link, capability or role, event, etc.) about an AR by a Sensor or other test tool.

- The PDP should be configured so that:
  - When an AR successfully connects to the network, the MAP Client on the PDP publishes metadata (MAC address, IP address, VLAN, other status, and/or optional identity/integrity information) to the MAP and searches for metadata on the AR.
  - When the MAP returns metadata to the PDP related to that AR, the PDP takes some action (e.g. provisions access, or disconnects or quarantines the AR via RADIUS CoA, depending upon the policy applied).
- An AR, PEP, and Sensor or test tool will generally be used in this test also but they are not the components under test.
  - If used, the AR and PEP should be configured to allow an authenticated AR to access the network, and the PEP should be configured to disconnect or quarantine the AR when instructed to do so by the PDP.

Test Steps:

- The AR is authenticated to the network or other steps are taken to cause the PDP to register an authenticated session.
- The PDP publishes metadata on the AR to the MAP and searches the MAP for metadata on that AR.
- The MAP returns metadata to the PDP as a result of the search.

Expected Outcome:

- When the PDP successfully authenticates the AR, it should publish metadata (MAC address, IP address, VLAN, other status, and/or optional identity/integrity information) to the MAP.
  - Measurement of this outcome is by observing or querying the MAP database to determine that metadata for that session is present.
- The PDP should search the MAP for metadata on that AR.
  - This outcome can be measured by using logs and/or packet captures to observe the messages sent between the PDP and the MAP.
- When the PDP receives the search result metadata from the MAP, it should apply the appropriate policy to the AR and send instructions to the PEP.
  - Measurement of this outcome is by observing the PDP logs, the status of the AR within the PDP, and the instructions sent from the PDP to the PEP.
  - If the PEP supports enforcement of permission, disconnect, or quarantine instructions received from the PDP, this outcome can also be measured by attempting to send traffic from the AR that would be permitted or denied under the instruction from the PDP and verifying that it is successful or unsuccessful, as appropriate.

Anticipated Failures:

- If the appropriate PDP-published metadata does not show up in the MAP after the AR successfully connects to the network, or the PDP does not successfully search for metadata within the MAP for that AR, or the PDP does not apply policy to the AR upon receiving the search result from the MAP, then either one of the preconditions has not been met or one or more of the PDP, MAP Client, or MAP Server has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the MAP Client and the MAP Server and/or the PDP and the PEP.

3.4.3 PDP Subscribe / Consume

This test case is required only for MAP Client implementations that support the ability to search for metadata, subscribe to identifiers, and consume notifications.

Preconditions:

- A PDP is acting as a MAP Client. A MAP Server is installed on a MAP.
- A Sensor or test tool capable of publishing metadata related to an AR (such as ip-mac link, capability or role, event, etc.) to the MAP is present.
- The PDP should be configured so that:
    - When an AR successfully connects to the network, the MAP Client on the PDP publishes metadata (MAC address, IP address, VLAN, other status, and/or optional identity/integrity information) to the MAP, searches for metadata on the AR, and subscribes to notifications from the MAP for that AR.
    - When the MAP notifies the PDP of updated metadata for that AR, the PDP consumes the notification applies policy to the AR and takes some action (e.g. provisions access, or disconnects or quarantines the AR via RADIUS CoA, depending upon the policy applied).
- An AR, PEP, and Sensor or test tool will generally be used in this test also but they are not the components under test.
    - If used, the AR and PEP should be configured to allow an authenticated AR to access the network, and the PEP should be configured to disconnect or quarantine the AR when instructed to do so by the PDP. The Sensor or test tool should be configured to publish metadata related to the AR.

Test Steps:

- The AR is authenticated to the network or other steps are taken to cause the PDP to register an authenticated session.
- The PDP publishes metadata on that AR to the MAP, searches the MAP for metadata on that AR, then subscribes to notifications from the MAP for that AR.
- The Sensor or test tool publishes metadata to the MAP for that AR, and the MAP notifies the PDP.

Expected Outcome:

- When the PDP successfully authenticates the AR, it should publish metadata (MAC address, IP address, VLAN, other status, and/or optional identity/integrity information) to the MAP.
    - Measurement of this outcome is by observing or querying the MAP database to determine that metadata for that session is present.
- The PDP should search the MAP for metadata on that AR, then subscribe to notifications from the MAP for that AR.
    - This outcome can be measured by using logs and/or packet captures to observe the messages sent between the PDP and the MAP. Also, if the MAP provides a mechanism for viewing its subscription list, measurement of this outcome is by observing or querying the MAP database to determine that the PDP is subscribed to notifications for that AR.
- When the PDP receives notification of the updated metadata from the MAP, it should apply the appropriate policy to the AR and send instructions to the PEP.

  - Measurement of this outcome is by observing the PDP logs, the status of the AR within the PDP, and the instructions sent from the PDP to the PEP.
  - If the PEP supports enforcement of permission, disconnect or quarantine instructions received from the PDP, this outcome can also be measured by attempting to send traffic from the AR that would be permitted or denied under the instruction from the PDP and verifying that it is successful or unsuccessful, as appropriate.

Anticipated Failures:

- If the appropriate PDP-published metadata does not show up in the MAP after the AR successfully connects to the network, or the PDP does not successfully subscribe to notifications from the MAP for that AR, or the PDP does not apply the appropriate policy to the AR upon receiving notification from the MAP, then either one of the preconditions has not been met or one or more of the PDP, MAP Client, or MAP Server has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the MAP Client and the MAP Server and/or the PDP and the PEP.

3.4.4 Sensor Publish / Delete (update)

Preconditions:

- A Sensor is acting as a MAP Client. A MAP Server is installed on a MAP.
- The Sensor should be configured so that when the Sensor detects activity related to an AR, the MAP Client on the Sensor publishes metadata (e.g. an ip-mac link) to the MAP using the update operation.
- An AR, PDP, and PEP will generally be used in this test also but they are not the components under test.
  - If used, the AR, PDP, and PEP should be configured to allow an authenticated AR to access the network.

Test Steps:

- The AR generates traffic or responds to investigation in a way that triggers an observation in the Sensor.
- The AR stops generating traffic, the response to investigation changes, or something else happens, and the Sensor observes the termination of that activity.

Expected Outcome:

- When the Sensor detects the AR traffic or investigation response that triggers the observation, it should publish metadata (e.g. ip-mac link) to the MAP.
  - Measurement of this outcome is by observing or querying the MAP database to determine that metadata for that observation is present.
- When the activity terminates, the Sensor should delete the metadata that it published for that observation.
  - Measurement of this outcome is by observing or querying the MAP database to determine that metadata for that observation is no longer present.

Anticipated Failures:

- If the appropriate metadata does not show up in the MAP after the observation is triggered, or remains in the MAP after the activity terminates, then either one of the preconditions has not been met or one or more of the Sensor, MAP Client, or MAP Server has malfunctioned.

  - To diagnose the problem, logs may be used to determine what messages were sent between the MAP Client and the MAP Server.

3.4.5 Sensor Publish (notify)

This test case is required only for IF-MAP implementations that support the IF-MAP Bindings for SOAP 2.0 specification.

Preconditions:

- A Sensor is acting as a MAP Client. A MAP Server is installed on a MAP.
- The Sensor should be configured so that when the Sensor detects an event related to an AR, the MAP Client on the Sensor publishes non-persistent metadata (e.g. event metadata) to the MAP using the notify operation.
- An AR, PDP, and PEP will generally be used in this test also but they are not the components under test.
  - If used, the AR, PDP, and PEP should be configured to allow an authenticated AR to access the network.

Test Steps:

- The AR generates traffic or responds to investigation in a way that triggers an event in the Sensor.

Expected Outcome:

- When the Sensor detects the AR traffic or investigation response that triggers the event, it should publish metadata (IP address, event type) to the MAP.
  - Measurement of this outcome is by observing or querying the MAP database to determine that metadata for that event is present.
- After subscribers have been notified, the MAP Server should not store the non-persistent metadata in its database.
  - Measurement of this outcome is by observing or querying the MAP database to determine that metadata for that event is no longer present.

Anticipated Failures:

- If the appropriate metadata does not show up in the MAP after the event is triggered, or remains in the MAP after subscribers have been notified, then either one of the preconditions has not been met or one or more of the Sensor, MAP Client, or MAP Server has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the MAP Client and the MAP Server.

3.4.6 Sensor Search / Consume

This test case is required only for MAP Client implementations that support the ability to search for metadata and apply policy based on search results.

Preconditions:

- A Sensor is acting as a MAP Client. A MAP Server is installed on a MAP.
- The MAP database is pre-populated with metadata (MAC address, IP address, capability or role, other status, and optional identity / integrity information) about an AR by a PDP or other test tool.
- The Sensor should be configured so that:

    - When the Sensor detects activity related to the AR, the MAP Client on the Sensor searches for metadata on the AR.
    - When the MAP returns metadata on the AR, the Sensor applies policy to the AR (e.g. monitoring profile, vulnerability profile, DHCP scope) based on that metadata.
- An AR, PDP, and PEP will generally be used in this test also but they are not the components under test.
    - If used, the AR, PDP, and PEP should be configured to allow an authenticated AR to access the network.

Test Steps:

- The AR generates traffic or responds to investigation in a way that triggers an observation in the Sensor.
- The Sensor searches the MAP for metadata on that AR.
- The MAP returns metadata to the Sensor as a result of the search.

Expected Outcome:

- When the Sensor detects activity related to the AR, the MAP Client on the Sensor should search the MAP for metadata related to that AR.
    - Measurement of this outcome is by observing logs and/or packet captures to determine the messages sent between the MAP Client and MAP Server.
- When the MAP Client on the Sensor receives the search result metadata from the MAP, the Sensor should apply the appropriate policy to the AR.
    - Measurement of this outcome is by observing the Sensor logs, the status of the AR within the Sensor, and any results of the policy applied to the AR by the Sensor.

Anticipated Failures:

- If the Sensor does not successfully search for metadata within the MAP for that AR, or the Sensor does not apply policy to the AR upon receiving the search result from the MAP, then either one of the preconditions has not been met or one or more of the Sensor, MAP Client, or MAP Server has malfunctioned.
    - To diagnose the problem, logs may be used to determine what messages were sent between the MAP Client and the MAP Server.

3.4.7 Sensor Subscribe / Consume

This test case is required only for MAP Client implementations that support the ability to search for metadata, subscribe to identifiers, and consume notifications.

Preconditions:

- A Sensor is acting as a MAP Client. A MAP Server is installed on a MAP.
- The MAP database is pre-populated with metadata (IP address, capability or role, other status, and optional identity / integrity information) about an AR by a PDP or other test tool. A second MAP Client or test tool publishes metadata related to the AR (such as ip-mac link, capability or role, event, etc.) during the course of the test.
- The Sensor should be configured so that:

    - When the Sensor detects an event related to the AR, the MAP Client on the Sensor searches for metadata on the AR and subscribes to notifications from the MAP for that AR.
    - When the MAP notifies the Sensor of an event published for that AR, the Sensor applies policy to the AR (e.g. monitoring profile, vulnerability profile, DHCP scope) based on that metadata.
- An AR, PDP, PEP, and second MAP Client or test tool will generally be used in this test also but they are not the components under test.
    - If used, the AR, PDP, and PEP should be configured to allow an authenticated AR to access the network. The second MAP Client or test tool should be configured to publish metadata related to the AR.

Test Steps:

- The AR generates traffic or responds to investigation in a way that triggers an event in the Sensor.
- The Sensor searches the MAP for metadata on that AR, then subscribes to notifications from the MAP for that AR.
- The second MAP Client or test tool publishes metadata to the MAP for that AR, and the MAP notifies the Sensor.

Expected Outcome:

- When the Sensor detects an event related to the AR, the MAP Client on the Sensor should search the MAP for metadata related to that AR, then subscribe to notifications from the MAP for that AR.
    - Measurement of this outcome is by observing logs and/or packet captures to determine the messages sent between the MAP Client and MAP Server. Also, if the MAP provides a mechanism for viewing its subscription list, measurement of this outcome is by observing or querying the MAP database to determine that the Sensor is subscribed to notifications for that AR.
- When the Sensor receives notification of the updated metadata from the MAP, the Sensor should apply the appropriate policy to the AR.
    - Measurement of this outcome is by observing the Sensor logs, the status of the AR within the Sensor, and any results of the policy applied to the AR by the Sensor.

Anticipated Failures:

- If the Sensor does not successfully subscribe to notifications from the MAP for that AR, or the Sensor does not take apply the appropriate policy to the AR upon receiving notification from the MAP, then either one of the preconditions has not been met or one or more of the Sensor, MAP Client, or MAP Server has malfunctioned.
    - To diagnose the problem, logs may be used to determine what messages were sent between the MAP Client and the MAP Server.

3.4.8 Flow Controller Search / Consume

Preconditions:

- A Flow Controller is acting as a MAP Client. A MAP Server is installed on a MAP.
- The MAP database is pre-populated with metadata (IP address, event, other status, and optional identity / integrity information) about an AR by a PDP and/or Sensor or other test tool(s).

- The Flow Controller should be configured so that:
    - When the Flow Controller detects activity related to the AR, the MAP Client on the Flow Controller searches for metadata on the AR.
    - When the MAP returns metadata on the AR, the Flow Controller applies policy to the AR and takes action (e.g. permit or deny traffic, depending upon the policy applied) based on that metadata.
- An AR, PDP, and PEP will generally be used in this test also but they are not the components under test.
    - If used, the AR, PDP, and PEP should be configured to allow an authenticated AR to access the network.

Test Steps:

- The AR attempts to send traffic through the Flow Controller.
- The Flow Controller searches the MAP for metadata on that AR.
- The MAP returns metadata to the Flow Controller as a result of the search.

Expected Outcome:

- When the AR attempts to send traffic through the Flow Controller, the MAP Client on the Flow Controller should search the MAP for metadata related to that AR.
    - Measurement of this outcome is by observing logs and/or packet captures to determine the messages sent between the MAP Client and MAP Server.
- When the MAP Client on the Flow Controller receives the search result metadata from the MAP, the Flow Controller should apply the appropriate policy to the AR and take action.
    - Measurement of this outcome is by observing the Flow Controller logs, the status of the AR within the Flow Controller, and whether the AR's traffic is permitted or denied by the Flow Controller.

Anticipated Failures:

- If the Flow Controller does not successfully search for metadata within the MAP for that AR, or the Flow Controller does not apply policy to the AR upon receiving the search result from the MAP, then either one of the preconditions has not been met or one or more of the Flow Controller, MAP Client, or MAP Server has malfunctioned.
    - To diagnose the problem, logs may be used to determine what messages were sent between the MAP Client and the MAP Server.

3.4.9 Flow Controller Subscribe / Consume

This test case is required only for MAP Client implementations that support the ability to search for metadata, subscribe to identifiers, and consume notifications.

Preconditions:

- A Flow Controller is acting as a MAP Client. A MAP Server is installed on a MAP.
- The MAP database is pre-populated with metadata (IP address, capability or role, other status, and optional identity / integrity information) about an AR by a PDP or other test tool. A second MAP Client test tool publishes metadata related to the AR (such as ip-mac link, capability or role, event, etc.) during the course of the test.
- The Flow Controller should be configured so that:

  - When the Flow Controller detects an event related to the AR, the MAP Client on the Flow Controller searches for metadata on the AR and subscribes to notifications from the MAP for that AR.
  - When the MAP notifies the Flow Controller of an event published for that AR, the Flow Controller applies policy to the AR and takes action (e.g. permit or deny traffic) based on that metadata.
- An AR, PDP, PEP, and second MAP Client or test tool will generally be used in this test also but they are not the components under test.
  - If used, the AR, PDP, and PEP should be configured to allow an authenticated AR to access the network. The second MAP Client or test tool should be configured to publish metadata related to the AR.

Test Steps:

- The AR attempts to send traffic through the Flow Controller.
- The Flow Controller searches the MAP for metadata on that AR, then subscribes to notifications from the MAP for that AR.
- The second MAP Client or test tool publishes metadata to the MAP for that AR, and the MAP notifies the Flow Controller.

Expected Outcome:

- When the AR attempts to send traffic through the Flow Controller, the MAP Client on the Flow Controller should search the MAP for metadata related to that AR, then subscribe to notifications from the MAP for that AR.
  - Measurement of this outcome is by observing logs and/or packet captures to determine the messages sent between the MAP Client and MAP Server. Also, if the MAP provides a mechanism for viewing its subscription list, measurement of this outcome is by observing or querying the MAP database to determine that the Flow Controller is subscribed to notifications for that AR.
- When the Flow Controller receives notification of the updated metadata from the MAP, the Flow Controller should apply the appropriate policy to the AR and take action.
  - Measurement of this outcome is by observing the Flow Controller logs, the status of the AR within the Flow Controller, and any results of the policy applied to the AR by the Flow Controller.

Anticipated Failures:

- If the Flow Controller does not successfully subscribe to notifications from the MAP for that AR, or the Flow Controller does not apply the appropriate policy to the AR upon receiving notification from the MAP, then either one of the preconditions has not been met or one or more of the PDP, MAP Client, or MAP Server has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the MAP Client and the MAP Server.

3.4.10 Other MAP Client Search / Consume

This test case is required only for other MAP Client implementations that support the ability to search for metadata and take action based on search results.

Preconditions:

- A network component is acting as a MAP Client. A MAP Server is installed on a MAP.

- The MAP database is pre-populated with metadata (IP address, capability or role, other status, and optional identity / integrity information) about an AR by a PDP or other test tool.
- The MAP Client should be configured so that:
  - When a query is initiated (such as a user searching for metadata related to an AR), the MAP Client searches for metadata related to the query.
  - When the MAP returns metadata on the AR, the MAP Client takes action based on the resulting metadata (e.g., displays the metadata graph).
- An AR, PDP, and PEP will generally be used in this test also but they are not the components under test.
  - If used, the AR, PDP, and PEP should be configured to allow an authenticated AR to access the network.

Test Steps:

- The querent initiates a request for metadata.
- The MAP Client searches the MAP for metadata related to the query.
- The MAP returns metadata to the MAP Client as a result of the search.

Expected Outcome:

- When the MAP Client receives a query, the MAP Client should search the MAP for metadata related to that query.
  - Measurement of this outcome is by observing logs and/or packet captures to determine the messages sent between the MAP Client and MAP Server.
- When the MAP Client receives the search result metadata from the MAP, the MAP Client should take action based on the resulting metadata.
  - Measurement of this outcome is by observing the MAP Client logs and/or any display presented by the MAP Client.

Anticipated Failures:

- If the MAP Client does not successfully search for metadata within the MAP related to the query, or the MAP Client does not take action upon receiving the search result from the MAP, then either one of the preconditions has not been met or one or more of the MAP Client or MAP Server has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the MAP Client and the MAP Server.

3.4.11 Other MAP Client Subscribe / Consume

This test case is required only for other MAP Client implementations that support the ability to search for metadata, subscribe to identifiers, and consume notifications.

Preconditions:

- A network component is acting as a MAP Client. A MAP Server is installed on a MAP.
- The MAP database is pre-populated with metadata (IP address, capability or role, other status, and optional identity / integrity information) about an AR by a PDP or other test tool. A Sensor or other test tool publishes metadata (such as an ip-mac link or event) during the course of the test.
- The MAP Client should be configured so that:

  - When a query is initiated (i.e., by a querent such as a user or application searching for metadata related to an AR), the MAP Client searches for metadata related to the query and subscribes to notifications from the MAP related to the query.
  - When the MAP notifies the MAP Client of a change in the metadata related the query, the MAP Client takes action (such as updating a display of the MAP graph) based on the notification.
- An AR, PDP, PEP, and Sensor will generally be used in this test also but they are not the components under test.
  - If used, the AR, PDP, and PEP should be configured to allow an authenticated AR to access the network.

Test Steps:

- The querent initiates a request for metadata.
- The MAP Client searches the MAP for metadata related to the query, then subscribes to notifications from the MAP related to that metadata.
- A Sensor or other test tool publishes metadata (such as an event or an ip-mac link) related to the query to the MAP, and the MAP notifies the MAP Client.

Expected Outcome:

- When the MAP Client receives a query, the MAP Client should search the MAP for metadata related to that query, then subscribe to notifications from the MAP for that metadata.
  - Measurement of this outcome is by observing logs and/or packet captures to determine the messages sent between the MAP Client and MAP Server. Also, if the MAP provides a mechanism for viewing its subscription list, measurement of this outcome is by observing or querying the MAP database to determine that the MAP Client is subscribed to notifications for that metadata.
- When the MAP Client receives notification of the event from the MAP, the MAP Client should take action (such as updating a display of the MAP graph) based on the notification.
  - Measurement of this outcome is by observing the MAP Client logs and/or any display presented by the MAP Client.

Anticipated Failures:

- If the MAP Client does not successfully subscribe to notifications from the MAP related to the query, or the MAP Client does not take action upon receiving the notification from the MAP, then either one of the preconditions has not been met or one or more of the MAP Client or MAP Server has malfunctioned.
  - To diagnose the problem, logs may be used to determine what messages were sent between the MAP Client and the MAP Server.

4 References

[1] Trusted Computing Group, *TNC IF-PEP for RADIUS Specification v1.1*, February 2007.

[2] Trusted Computing Group, *TNC IF-IMC Specification v1.2*, February 2007.

[3] Trusted Computing Group, *TNC IF-IMV Specification v1.2*, February 2007.

[4] Trusted Computing Group, *Compliance_TNC Compliance and Interoperability Principles, Specification Version 1.1, Draft Specification*, November 2010.

[5] Trusted Computing Group, *TNC Architecture for Interoperability*, Specification Version 1.4, May 2009.

[6] Trusted Computing Group, *TNC IF-TNCCS v1.2,* May 2009.

[7] Trusted Computing Group, *TNC IF-TNCCS: Protocol Bindings for SOH v1.0*, May 2007.

[8] Trusted Computing Group, *TNC IF-MAP Binding for SOAP v1.1*, May 2009.

[9] Trusted Computing Group, *TNC IF-MAP Binding for SOAP v2.0*, October 2011.

[10] Trusted Computing Group, *TNC IF-MAP Metadata for Network Security v1.0*, September 2010.