TCG Compliance_TNC IF-PEP Compliance Test Plan

Version 1.00
Revision 0.21
8 December 2008
Published

Contact:
admin@trustedcomputinggroup.org

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.

No license, express, implied, by estoppels, or otherwise, to any TCG or TCG member intellectual property rights is granted herein.

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide specific requirements for the compliance tests for IF-PEP for RADIUS v1.0. In particular, it defines and lists all the compliance test cases that must be passed to prove Compliance with respect to the IF-PEP for RADIUS v1.0 specification [2]. This document does not contain any normative statements.

1.2 Scope and Audience

The intended audience for this document includes test designers and implementers, as well as product developers and customers who need to understand the IF-PEP for RADIUS v1.0 compliance tests. Readers should be familiar with the TNC Architecture [1], with the Compliance_TNC Compliance and Interoperability Principles specification [3] and with IF-PEP for RADIUS v1.0.

2 Specifications and Components

2.1 Specifications

This document is based on the IF-PEP for RADIUS v1.0 specification [2] on the Compliance_TNC Compliance and Interoperability Principles document [1], and on RFC 2865 [4], RFC 2868 [5], RFC 3579 [6], RFC 3576 [7], and RFC 3580 [8]. The IF-PEP v1.0 specification defines the IF-PEP interface. The Compliance_TNC Compliance and Interoperability Principles document provides an overview of the Compliance_TNC testing. The referenced RFCs define aspects of the RADIUS protocol and attributes.

2.2 Components

There are two sets of IF-PEP compliance tests that test the two kinds of components that interface with IF-PEP: Policy Enforcement Point and Network Access Authority.

2.2.1 Policy Enforcement Points (PEPs)

The IF-PEP Compliance tests for Policy Enforcement Points (PEPs) tests that a PEP properly implements IF-PEP. The Test Target for this test is a PEP.

To test a PEP’s compliance with IF-PEP for RADIUS, a sequence of RADIUS exchanges must be conducted with the PEP. After each exchange, test traffic shall be sent to ensure that the test criteria are met and the PEP has properly implemented the type of network access directed by the PDP.

2.2.2 Network Access Authorities (NAAs)

The IF-PEP Compliance test for Network Access Authorities (NAAs) tests that an NAA properly implements IF-PEP. The Test Target for this test is an NAA.

To test a PDP’s compliance with IF-PEP for RADIUS, a sequence of RADIUS exchanges must be conducted with the NAA. After each exchange, traffic between the NAA and the PEP should be carefully examined to ensure that it complies with the IF-PEP for RADIUS specification.

3 Requirements and Recommendations

The IF-PEP v1.0 specification includes many requirements and recommendations for Policy Enforcement Points and Network Access Authorities. This section lists only the mandatory requirements since the compliance tests for IF-PEP only test normative requirements (not recommendations).

This section has three subsections. The first section lists mandatory requirements upon Policy Enforcement Points, which are tested by the IF-PEP compliance test for PEPs. The second section lists mandatory requirements upon Network Access Authorities, which are tested by the IF-PEP compliance test for NAAs. The third section lists other requirements that will not be tested by this test plan.

As required by the TCG Compliance and Interoperability Guidelines, each requirement listed below has a unique name composed of the string "CTNC" (for Compliance_TNC), "IFPEP1.0" (indicating that these are requirements from IF-PEP v1.0), "PEP" or "NAA" depending on which component the requirement applies to, a requirement number unique within the preceding prefix, "REQ" indicating it is a requirement, and a compliance classifier ("M" for MUST, "S" for SHOULD, "O" for OPTIONAL or MAY, "X" for Expressly Forbidden or MUST NOT). Usage classifiers are not included in requirement names at this time.

3.1 Requirements on PEPs

[CTNC-IFPEP1.0-PEP-REQ-1-M] A PEP MUST support at least one of the three isolation techniques consisting of either binary-, vlan-, and filter-based isolation. All RADIUS PEPs support binary isolation. Other isolation techniques are optional.

[CTNC-IFPEP1.0-PEP-REQ-2-M] A PEP MUST allow dynamic access policy update. This dynamic policy update may be via one of a number of methods, such as Change of Authorization (CoA), RADIUS Filter-Id support, or user re-authentication. There is no specific test case for this requirement.

[CTNC-IFPEP1.0-PEP-REQ-3-M] If a PEP supports VLAN-based isolation, it MUST support the RFC2868 tunnel attributes enumerated in section 5.3.2 of IF-PEP 1.0 and RFC3580 section 3.31 usage guidelines.

[CTNC-IFPEP1.0-PEP-REQ-4-M] If a PEP supports Filter-based isolation, it MUST support the Filter-ID attribute as defined in RFC2865 section 5.11 and RFC 3580 section 3.9 usage guidelines.

[CTNC-IFPEP1.0-PEP-REQ-5-M] If a PEP supports dynamic policy changes (as described in section 5.4 of IF-PEP), it MUST support RFC3576. We note that Service-Type of Authorize Only is not part of IF-PEP, so we do not have test cases for it. IPsec replay protection is also omitted because it is not used in the IF-PEP 1.0 specification.

[CTNC-IFPEP1.0-PEP-REQ-6-M] A PEP MUST support usage of non-obvious RADIUS secrets as described in RFC2865.

[CTNC-IFPEP1.0-PEP-REQ-7-M] A PEP MUST support Message-Authenticator attribute as described in RFC3579, section 3.1.

RFC2865 related requirements:

[CTNC-IFPEP1.0-PEP-REQ-8-M] A NAS [PEP] that does not implement a given service MUST NOT implement RADIUS attributes for that service. (RFC 2865, section 1.1) [The term "service" as used in this requirement refers to services identified by a Service-Type attribute.]

[CTNC-IFPEP1.0-PEP-REQ-9-M] A NAS [PEP] MUST treat a RADIUS Access-Accept authorizing an unavailable service as an Access-Reject instead. (RFC 2865, section 1.1) [The term “service” as used in this requirement refers to services identified by a Service-Type attribute.]

[CTNC-IFPEP1.0-PEP-REQ-10-M] If the NAS [PEP] is retransmitting a RADIUS request to the same server as before, and the attributes have not changed, the PEP MUST use the same Request Authenticator, ID, and source port. If any attributes have changed, the PEP MUST use a new Request Authenticator and ID. (RFC 2865, section 2.5)

[CTNC-IFPEP1.0-PEP-REQ-11-M] Octets outside the range of the Length field MUST be treated as padding and ignored on reception.

[CTNC-IFPEP1.0-PEP-REQ-12-M] If the packet is shorter than the Length field indicates, it MUST be silently discarded. The minimum Length is 20 and maximum Length is 4096. (RFC 2865, section 3)

[CTNC-IFPEP1.0-PEP-REQ-13-M] A system [PEP] wishing to authenticate a user MUST transmit a RADIUS packet with the Code field set to 1 (Access-Request). (RFC 2865, section 4.1)

[CTNC-IFPEP1.0-PEP-REQ-14-M] An Access-Request MUST contain either a NAS-IP-Address attribute or a NAS-Identifier attribute. It MAY contain both (RFC 2865, section 4.1)

[CTNC-IFPEP1.0-PEP-REQ-15-M] An Access-Request MUST contain either a User-Password or a CHAP-Password or a State attribute. An Access-Request MUST NOT contain both a User-Password and a CHAP-Password. (RFC 2865, section 4.1) [This requirement is qualified by the following sentence in RFC 2865, which says “If future extensions allow other kinds of authentication information to be conveyed, the attribute for that can be used in an Access-Request instead of User-Password or CHAP-Password.” RFC 3579 further states “An Access-Request that contains either a User-Password or CHAP-Password or ARAP-Password or one or more EAP-Message attributes MUST NOT contain more than one type of those four attributes.” Since EAP is always used for TNC handshakes over RADIUS, requirement [CTNC-IFPEP1.0-PEP-REQ-15-M] does not apply to TNC and therefore no test is included for it in this test suite.]

[CTNC-IFPEP1.0-PEP-REQ-16-M] The Identifier field of an Access-Request MUST be changed whenever the content of the Attributes field changes, and whenever a valid reply has been received for a previous request.

[CTNC-IFPEP1.0-PEP-REQ-17-M] For retransmissions, the Identifier MUST remain unchanged. (RFC 2865, section 4.1)

[CTNC-IFPEP1.0-PEP-REQ-18-M] The Request Authenticator value [of an Access-Request] MUST be changed each time a new Identifier is used. (RFC 2865, section 4.1)

[CTNC-IFPEP1.0-PEP-REQ-19-M] If a NAS [PEP] does not support challenge/response, it MUST treat an Access-Challenge as though it had received an Access-Reject instead. (RFC 2865, section 4.4) [Because all TNC handshakes over RADIUS use EAP, which requires support for challenge-response, this requirement does not apply. Therefore no tests are included for it.]

[CTNC-IFPEP1.0-PEP-REQ-20-M] A RADIUS server or client MUST NOT have any dependencies on the order of attributes of different types. A RADIUS server or client MUST NOT require attributes of the same type to be contiguous. (RFC 2865, section 5.0)

[CTNC-IFPEP1.0-PEP-REQ-21-M] If an Attribute is received in an Access-Accept, Access-Reject or Access-Challenge packet with an invalid Attribute length, the packet MUST either be treated as an Access-Reject or else silently discarded. (RFC 2865, section 5.0)

[CTNC-IFPEP1.0-PEP-REQ-22-M] The Value field is one or more octets and contains information specific to the Attribute. The format and length of the Value field is determined by the Type and Length fields. Note that none of the types in RADIUS terminate with a NUL (hex 00). In particular, types "text" and "string" in RADIUS do not terminate with a NUL (hex 00). The Attribute has a length field and does not use a terminator. Text contains UTF-8 encoded 10646 characters and String contains 8-bit binary data. Servers and servers and clients MUST be able to deal with embedded nulls. (RFC 2865, section 5.0)

[CTNC-IFPEP1.0-PEP-REQ-23-M] If the Value field is of Text type, then Text of length zero MUST NOT be sent. (RFC 2865, section 5.0)

[CTNC-IFPEP1.0-PEP-REQ-24-M] If the Value field is of String type, then String of length zero MUST NOT be sent. (RFC 2865, section 5.0)

[CTNC-IFPEP1.0-PEP-REQ-25-M] This attribute User-Name indicates the name of the user to be authenticated. It MUST be sent in Access-Request packets if available. (RFC 2865, section 5.1)

[CTNC-IFPEP1.0-PEP-REQ-26-M] The Filter-Id Text field is one or more octets, and it's contents are implementation dependent. It is intended to be human readable and MUST NOT affect operation of the protocol. (RFC 2865, section 5.11)

[CTNC-IFPEP1.0-PEP-REQ-27-M] Multiple Reply-Message's MAY be included and if any are displayed, they MUST be displayed in the same order as they appear in the packet. (RFC 2865, section 5.18) [No test for this requirement is included in this test suite because RFC 3579 says the Reply-Message attribute MUST NOT be used with EAP and TNC always uses EAP when IF-PEP for RADIUS is used.]

[CTNC-IFPEP1.0-PEP-REQ-28-M] The Reply-Message Text field is one or more octets, and its contents are implementation dependent. It is intended to be human readable, and MUST NOT affect operation of the protocol. (RFC 2865, section 5.18) [No test for this requirement is included in this test suite because RFC 3579 says the Reply-Message attribute MUST NOT be used with EAP and TNC always uses EAP when IF-PEP for RADIUS is used.]

[CTNC-IFPEP1.0-PEP-REQ-29-M] The Framed-Route Text field is one or more octets, and it's contents are implementation dependent. It is intended to be human readable and MUST NOT affect operation of the protocol. (RFC 2865, section 5.22)

[CTNC-IFPEP1.0-PEP-REQ-30-M] The State attribute is available to be sent by the server to the client in an Access-Challenge and MUST be sent unmodified from the client to the server in the new Access-Request reply to that challenge, if any. The client MUST NOT interpret the attribute locally. (RFC 2865, section 5.24)

[CTNC-IFPEP1.0-PEP-REQ-31-M] The State attribute is available to be sent by the server to the client in an Access-Accept that also includes a Termination-Action Attribute with the value of RADIUS-Request. If the NAS performs the Termination-Action by sending a new Access-Request upon termination of the current session, it MUST include the State attribute unchanged in that Access-Request. (RFC 2865, section 5.24) [This is not widely implemented or essential to IF-PEP so no test case is included for it.]

[CTNC-IFPEP1.0-PEP-REQ-32-M] The client MUST NOT interpret the Class attribute locally. (RFC 2865, section 5.25)

[CTNC-IFPEP1.0-PEP-REQ-33-M] The Vendor-Specific Attribute MUST not affect the operation of the RADIUS protocol. (RFC 2865, section 5.26)

[CTNC-IFPEP1.0-PEP-REQ-34-M] A PEP MUST not use the Framed-Routing, Filter-Id, Login-Service, Login-TCP-Port, Reply-Message, Callback-Id, Framed-Route, Framed-IPX-Network, Class, Session-Timeout, Idle-Timeout, Termination-Action, Framed-AppleTalk-Link, Framed-AppleTalk-Network and Framed-AppleTalk-Zone attributes in

Access-Request packets. A PEP MUST not use more than one instance of the following attributes in Access-Request packets, User-Name, Service-Type, Framed-Protocol, Framed-IP-Address, Framed-IP-Netmask, Framed-MTU, Callback-Number, State, Login-LAT-Service, Login-LAT-Node, Login-LAT-Group, Port-Limit and Login-LAT-Port. (RFC 2865, section 5.44)

RFC2868 related requirements:

[CTNC-IFPEP1.0-PEP-REQ-35-M] If a tunnel initiator receives an Access-Accept packet which contains only unknown or unsupported Tunnel-Types, the tunnel initiator MUST behave as though an Access-Reject had been received instead. (RFC 2868, Section 3.1)

[CTNC-IFPEP1.0-PEP-REQ-36-M] If the Tag field is unused in the Tunnel-Type attribute, it MUST be zero. (RFC 2868, Section 3.1) [We have a test case to verify that the PEP can handle zero tag values.]

[CTNC-IFPEP1.0-PEP-REQ-37-M] If a tunnel initiator receives an Access-Accept packet which contains only unknown or unsupported Tunnel-Medium-Types, the tunnel initiator MUST behave as though as Access-Reject had been received instead. (RFC 2868, Section 3.2)

[CTNC-IFPEP1.0-PEP-REQ-38-M] If the Tag field is unused in the Tunnel-Medium-Type attribute, it MUST be zero. (RFC 2868, Section 3.2) [We have a test case to verify that the PEP can handle zero tag values.]

RFC3576 related requirements:

[CTNC-IFPEP1.0-PEP-REQ-39-M] A NAS MUST respond to a Disconnect-Request including a Service-Type Attribute with an unsupported value with a Disconnect-NAK (RFC 3576, section 2.2).

[CTNC-IFPEP1.0-PEP-REQ-40-M] A NAS MUST respond to a CoA-Request including a Service-Type Attribute with an unsupported value with a CoA-NAK. (RFC 3576, section 2.2)

[CTNC-IFPEP1.0-PEP-REQ-41-M] A NAS MUST respond to a CoA-Request containing one or more unsupported Attributes or Attribute values with a CoA-NAK. (RFC 3576, section 2.3)

[CTNC-IFPEP1.0-PEP-REQ-42-M] A Disconnect-Request containing one or more unsupported Attributes or Attribute values MUST be answered with a Disconnect-NAK. (RFC 3576, section 2.3)

[CTNC-IFPEP1.0-PEP-REQ-43-M] All NAS identification attributes included in a Request message MUST match in order for a Disconnect-Request or CoA-Request to be successful. (RFC 3576, section 3)

[CTNC-IFPEP1.0-PEP-REQ-44-M] For session identification attributes, the User-Name and Acct-Session-Id Attributes, if included, MUST match in order for a Disconnect-Request or CoA-Request to be successful. (RFC 3576, section 3)

[CTNC-IFPEP1.0-PEP-REQ-45-M] The Error-Cause attribute values of 200-299 represent successful completion, and can only be sent within Disconnect-ACK or CoA-ACK message. An Error-Cause attribute with these values MUST NOT be sent within a Disconnect-NAK or CoA-NAK. (RFC 3576, section 3)

[CTNC-IFPEP1.0-PEP-REQ-46-M] Error-Cause attribute values of 400-499 represent fatal errors committed by the RADIUS server, and MUST NOT be sent within CoA-ACK or Disconnect-ACK messages. (RFC 3576, section 3)

[CTNC-IFPEP1.0-PEP-REQ-47-M] Error-Cause attribute values of Values 500-599 represent fatal errors occurring on a NAS or RADIUS proxy, and MUST NOT be sent within CoA-ACK or Disconnect-ACK messages. (RFC 3576, section 3)

[CTNC-IFPEP1.0-PEP-REQ-48-M] The State Attribute is available to be sent by the RADIUS server to the NAS in a Disconnect-Request or CoA-Request message and MUST be sent unmodified from the NAS to the RADIUS server in a subsequent ACK or NAK message. (RFC 3576, section 3.2)

[CTNC-IFPEP1.0-PEP-REQ-49-M] A NAS [PEP] or RADIUS proxy MUST silently discard Disconnect-Request or CoA-Request messages from untrusted sources. (RFC 3576, section 5.1)

3.2 Requirements on NAAs

[CTNC-IFPEP1.0-NAA-REQ-1] An NAA MUST support at least one of the three isolation techniques consisting of either binary-, vlan-, and filter-based isolation.

[CTNC-IFPEP1.0-NAA-REQ-2] An NAA MUST allow dynamic access policy update. This dynamic policy update may be via one of a number of methods, such as Change of Authorization (CoA), RADIUS Filter-Id support, or user re-authentication.

[CTNC-IFPEP1.0-NAA-REQ-3] If an NAA supports VLAN-based isolation, it MUST support RFC2868 tunnel attributes in sections 3.1, 3.2, and 3.6 and RFC3580 section 3.31 usage guidelines.

[CTNC-IFPEP1.0-NAA-REQ-4] If an NAA supports Filter-based isolation, it MUST support the Filter-ID attribute as defined in RFC2865 and RFC3580 section 3.9 usage guidelines.

[CTNC-IFPEP1.0-NAA-REQ-5] If a NAA supports dynamic policy changes (as described in section 5.4 of IF-PEP), it MUST support RFC3576.

[CTNC-IFPEP1.0-NAA-REQ-6] An NAA MUST support usage of non-obvious RADIUS secrets as described in RFC2865.

[CTNC-IFPEP1.0-NAA-REQ-7] An NAA MUST support Message-Authenticator attribute as described in RFC3579, section 3.1.

RFC2865 related requirements:

[CTNC-IFPEP1.0-NAA-REQ-8] A request from a client for which the RADIUS server does not have a shared secret MUST be silently discarded. (RFC 2865, section 2)

[CTNC-IFPEP1.0-NAA-REQ-9] If the RADIUS server [NAA] is unable to perform the requested authentication, it MUST return an Access-Reject. (RFC 2865, section 2.2)

[CTNC-IFPEP1.0-NAA-REQ-10] Octets outside the range of the Length field MUST be treated as padding and ignored on reception. (RFC 2865, section 3)

[CTNC-IFPEP1.0-NAA-REQ-11] If the packet is shorter than the Length field indicates, it MUST be silently discarded. (RFC 2865, section 3)

[CTNC-IFPEP1.0-NAA-REQ-12] A RADIUS server [NAA] MUST use the source IP address of the RADIUS UDP packet to decide which shared secret to use, so that RADIUS requests can be proxied. (RFC 2865, section 3)

[CTNC-IFPEP1.0-NAA-REQ-13] Upon receipt of an Access-Request from a valid client [PEP], an appropriate reply MUST be transmitted. (RFC 2865, section 4.1) An appropriate response is: Access-Accept, Access-Challenge, Access-Reject.

[CTNC-IFPEP1.0-NAA-REQ-14] If all attribute values received in an Access-Request are acceptable then the RADIUS implementation [NAA] MUST transmit a packet with the Code field set to 2 (Access-Accept). (RFC 2865, section 4.2)

[CTNC-IFPEP1.0-NAA-REQ-15] On reception of an Access-Accept, the Identifier field is matched with a pending Access-Request. The Response Authenticator field [of an Access-Accept]

MUST contain the correct response for the pending Access-Request. (RFC 2865, section 4.2)

[CTNC-IFPEP1.0-NAA-REQ-16] If any value of the received Attributes [of an Access-Request] is not acceptable, then the RADIUS server [NAA] MUST transmit a packet with the Code field set to 3 (Access-Reject). (RFC 2865, section 4.3)

[CTNC-IFPEP1.0-NAA-REQ-17] If the RADIUS server [NAA] desires to send the user a challenge requiring a response, then the RADIUS server [NAA] MUST respond to the Access-Request by transmitting a packet with the Code field set to 11 (Access-Challenge). (RFC 2865, section 4.4)

[CTNC-IFPEP1.0-NAA-REQ-18] If the RADIUS server [NAA] sends an Access-Challenge, the Identifier field MUST match that of a pending Access-Request. Additionally, the Response Authenticator field MUST contain the correct response for the pending Access-Request. (RFC 2865, section 4.4)

[CTNC-IFPEP1.0-NAA-REQ-19] A RADIUS server [NAA] or client MUST NOT have any dependencies on the order of attributes of different types. A RADIUS server [NAA] or client MUST NOT require attributes of the same type to be contiguous. (RFC 2865, section 5.0)

[CTNC-IFPEP1.0-NAA-REQ-20] If an Attribute is received in an Access-Accept, Access-Reject or Access-Challenge packet with an invalid Attribute length, the packet MUST either be treated as an Access-Reject or else silently discarded. (RFC 2865, section 5.0)

[CTNC-IFPEP1.0-NAA-REQ-21] The Value field is one or more octets and contains information specific to the Attribute. The format and length of the Value field is determined by the Type and Length fields. Note that none of the types in RADIUS terminate with a NUL (hex 00). In particular, types "text" and "string" in RADIUS do not terminate with a NUL (hex 00). The Attribute has a length field and does not use a terminator. Text contains UTF-8 encoded 10646 characters and String contains 8-bit binary data. Servers and servers and clients MUST be able to deal with embedded nulls. (RFC 2865, section 5.0)

[CTNC-IFPEP1.0-NAA-REQ-22] If the Value field is of Text type, then Text of length zero MUST NOT be sent. (RFC 2865, section 5.0)

[CTNC-IFPEP1.0-NAA-REQ-23] If the Value field is of String type, then String of length zero MUST NOT be sent. (RFC 2865, section 5.0)

[CTNC-IFPEP1.0-NAA-REQ-24] Note that NAS-IP-Address MUST NOT be used to select the shared secret used to authenticate the request. The source IP address of the Access-Request packet MUST be used to select the shared secret. (RFC 2865, section 5.4)

[CTNC-IFPEP1.0-NAA-REQ-25] It [Vendor-Specific Attribute] MUST not affect the operation of the RADIUS protocol. Servers not equipped to interpret the vendor-specific information sent by a client MUST ignore it (although it may be reported). (RFC 2865, section 5.26)

[CTNC-IFPEP1.0-NAA-REQ-26] Note that NAS-Identifier MUST NOT be used to select the shared secret used to authenticate the request. The source IP address of the Access-Request packet MUST be used to select the shared secret. (RFC 2865, section 5.32)

[CTNC-IFPEP1.0-NAA-REQ-27] A RADIUS server [NAA] MUST follow the attribute usage guide as defined in Table 5.44 in RFC 2865 when placing attributes in packets. An NAA MUST not use the State, Vendor-Specific, Session-Timeout and Idle-Timeout attributes in Access-Reject packets.

An NAA MUST not use the User-Name, Service-Type, Framed-Protocol, Framed-IP-Address, Framed-IP-Netmask, Framed-Routing, Filter-Id, Framed-MTU, Framed-Compression, Login-IP-Host, Login-Service, Login-TCP-Port, Callback-Number, Callback-Id, Framed-Route, Framed-IPX-Network, Class, Termination-Action, Login-LAT-Service, Login-LAT-Node, Login-LAT-Group, Framed-AppleTalk-Link, Framed-AppleTalk-

Network, Framed-AppleTalk-Zone, Port-Limit and Login-LAT-Port attributes in Access-Reject and Access-Challenge packets.

An NAA MUST not use the User-Password, CHAP-Password, NAS-IP-Address NAS-Port, Called-Station-Id, Calling-Station-Id, NAS-Identifier, CHAP-Challenge and NAS-Port-Type attributes in Access-Accept, Access-Reject and Access-Challenge packets.

An NAA MUST not use more than one instance of the following attributes in Access-Accept packets, User-Name, Service-Type, Framed-Protocol, Framed-IP-Address, Framed-IP-Netmask, Framed-MTU, Callback-Number, State, Login-LAT-Service, Login-LAT-Node, Login-LAT-Group, Port-Limit and Login-LAT-Port.

An NAA MUST not use more than one instance of the following attributes in Access-Request packets, User-Password, CHAP-Password, NAS-IP-Address, NAS-Port, Called-Station-Id, Calling-Station-Id, NAS-Identifier, CHAP-Challenge and NAS-Port-Type.

An NAA MUST not use more than one instance of the following attributes in Access-Accept packets, Frame-Routing, Callback-Id, Framed-IPX-Network, Session-Timout, Idle-Timeout, Termination-Action, Framed-AppleTalk-Link and Framed-AppleTalk-Zone. An NAA MUST not use more than one instance of the following attributes in Access-Challenge packets, State, Session-Timeout and Idle-Timeout. (RFC 2865, section 5.44)

An NAA MUST not use any forbidden access reject packet attributes per table 5.44 of RFC 2865.

RFC2868 related requirements:

[CTNC-IFPEP1.0-NAA-REQ-28] If the Tag field is unused in the Tunnel-Type attribute, it MUST be zero. (RFC 2868, Section 3.1) [Some old PEPs require the Tag field to be non-zero when it is not used, in spite of this requirement. Therefore, NAAs may choose allow local configuration to enable non-zero values when the Tag field is unused. However, the default should be to send zero Tag values when the Tag field is unused.]

[CTNC-IFPEP1.0-NAA-REQ-29] If the Tag field is unused in the Tunnel-Medium-Type attribute, it MUST be zero. (RFC 2868, Section 3.2) [Some old PEPs require the Tag field to be non-zero when it is not used, in spite of this requirement. Therefore, NAAs may choose allow local configuration to enable non-zero values when the Tag field is unused. However, the default should be to send zero Tag values when the Tag field is unused.]

3.3 Other Requirements

Requirements listed in this section are requirements for neither PEP nor NAA. They are listed here for completeness. However, they are out of scope and we will not provide test cases.

[CTNC-IFPEP1.0-OTHER-1] If any Proxy-State attributes were present in the Access-Request, they MUST be copied unmodified and in order into the response packet. (RFC 2865, section 2)

[CTNC-IFPEP1.0-OTHER-2] The forwarding server MUST treat any Proxy-State attributes already in the packet as opaque data. It's operation MUST NOT depend on the content of Proxy-State attributes added by previous servers. (RFC 2865, section 2.3)

[CTNC-IFPEP1.0-OTHER-3] If a CHAP-Password attribute is present in the packet and no CHAP-Challenge attribute is present, the forwarding server MUST leave the Request-Authenticator untouched or copy it to a CHAP-Challenge attribute. (RFC 2865, section 2.3)

[CTNC-IFPEP1.0-OTHER-4] The forwarding server MAY add one Proxy-State attribute to the packet. It MUST NOT add more than one. If it adds a Proxy-State, the Proxy-State MUST appear after any other Proxy-States in the packet. The forwarding server MUST NOT modify any other Proxy-States that were in the packet. It may choose not to forward them, but it MUST NOT change their contents. The forwarding server MUST NOT change the order of any attributes of the same type, including Proxy-State. (RFC 2865, section 2.3)

[CTNC-IFPEP1.0-OTHER-5] The remote server MUST copy all Proxy-State attributes in order from the Access-Request to the response packet, without modifying them. (RFC 2865, section 2.3)

[CTNC-IFPEP1.0-OTHER-6] A forwarding server MUST not modify existing Proxy-State, State, or Class attributes present in the packet. (RFC 2865, section 2.3)

[CTNC-IFPEP1.0-OTHER-7] When using a forwarding proxy, the proxy must be able to alter the packet as it passes through in each direction - when the proxy forwards the request, the proxy MAY add a Proxy-State Attribute, and when the proxy forwards a response, it MUST remove it's Proxy-State Attribute if it added one. (RFC 2865, section 3)

[CTNC-IFPEP1.0-OTHER-8] A NAS which supports PAP MAY forward the Reply-Message to the NAS and accept a PAP response which it can use as though the user had entered the response. If the NAS cannot do so, it MUST treat the Access-Challenge as though it had received an Access-Reject instead. (RFC 2865, section 4.4)

[CTNC-IFPEP1.0-OTHER-9] If multiple Attributes with the same Type are present, the order of Attributes with the same Type MUST be preserved by any proxies. (RFC 2865, section 5)

[CTNC-IFPEP1.0-OTHER-10] The Proxy State attribute is available to be sent by a proxy server to another server when forwarding an Access-Request and MUST be returned unmodified in the Access-Accept, Access-Reject or Access-Challenge. When the proxy server receives the response to its request, it MUST remove its own Proxy-State (the last Proxy-State in the packet) before forwarding the response to the NAS. If a Proxy-State Attribute is added to a packet when forwarding the packet, the Proxy-State Attribute MUST be added after any existing Proxy-State attributes. The content of any Proxy-State other than the one added by the current server should be treated as opaque octets and MUST NOT affect operation of the protocol. (RFC 2865, section 5.33)

4 Configurations and Topologies

4.1 Common Setup

Access Requestor

An Access Requestor will be needed to request access to certain networks or services. This Access Requestor should make properly formatted requests and actions to simulate a valid test requirement. It is assumed that all required parameters involved are configurable on this device.

Network Analyzers

Network analyzers are used to validate the results of each test. The network analyzers used for this test plan will have the ability to capture traffic transmitted over the network at designated spots, and possess the ability to interpret and verify that traffic. Wireshark (Ethereal) is an open source tool that can do this. It also includes RADIUS encode/decode libraries.

RADIUS Simulator

RADIUS simulators are used for attribute testing. The RADIUS simulator must be able to generate a RADIUS exchange, acting as either a PEP or an NAA, with specific customized attributes.

Policy Enforcement Point (PEP)

The Policy Enforcement Point (PEP) may be an 802.1X-capable switch or wireless access point.

Network Access Authority (NAA)

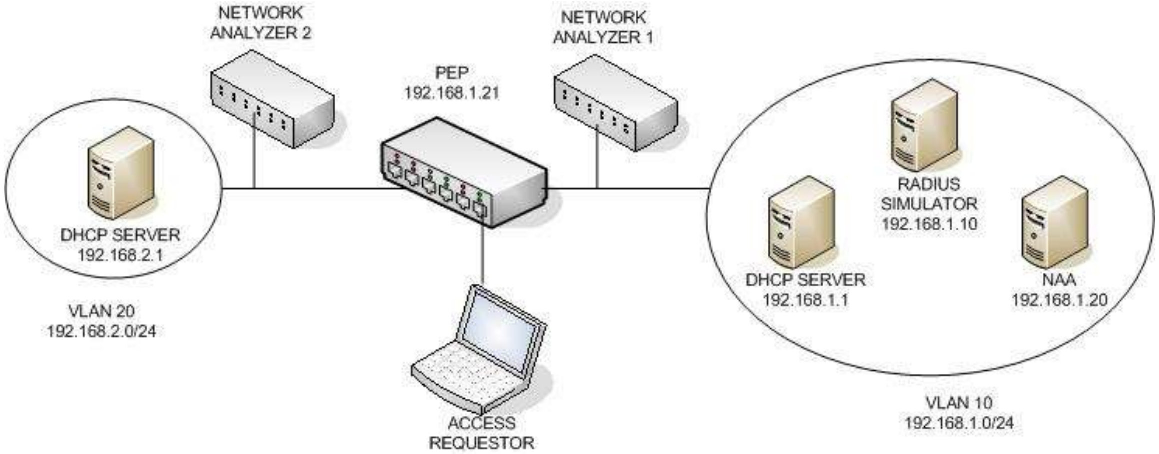
The Network Access Authority decides what network access should be granted to the Access Requestor (if any) and communicates the results of its decision to the PEP. The NAA is a RADIUS server. In the cases where the NAA is not the device under test, the NAA must respond to pings to enable connectivity tests.

DHCP Servers

The DHCP server with IP address 192.168.2.1 assigns addresses in 192.168.2.0/24. The DHCP server with IP address 192.168.1.1 assigns addresses in 192.168.1.0/24. Both must respond to pings to enable connectivity tests.

4.1.1 Test Topology

The test topology depicted below is used for all test cases. For the NAA test cases, only traffic between the PEP and the NAA (Network Analyzer 1) must be analyzed. For the PEP test cases, traffic within both VLANs must be analyzed.



Two VLANs are used in this topology:

VLAN 10	192.168.1.0/24
VLAN 20	192.168.2.0/24

If the PEP doesn't support dynamic VLAN assignment, VLAN 20 and all components on it can be omitted. No router or VLAN bridge is included in the test topology, so traffic cannot flow from VLAN 10 to VLAN 20. VLAN 10 MUST be used as the default VLAN (PVID / native VLAN) for PEP ports.

The following address assignments are used:

- 192.168.1.1 - VLAN 10 DHCP server
- 192.168.1.10 - RADIUS Simulator
- 192.168.1.20 - RADIUS server (NAA)
- 192.168.1.21 - switch / AP (PEP)
- 192.168.2.1 - VLAN 20 DHCP server

Network Analyzer 1 (right) analyzes traffic between the PEP and VLAN 10. RADIUS Simulator generates or replays traffic onto VLAN 10. Network Analyzer 2 (left) analyzes traffic between the PEP and VLAN 20.

All devices MUST have consistent time and date. The test topology MUST be reset to default configuration at the start of every test case.

The PEP must be configured to use the NAA as its RADIUS server. The NAA must be configured to recognize the PEP as a RADIUS client. Configure the PEP so that if an Access-Accept is received, access will be provided, and if an Access-Reject is received, no access will be provided. This is referred to as "binary isolation".

The PEP must be further configured as follows:

- Manually disable port access control (802.1X) for NAA, network analyzer and RADIUS simulator ports
  - *AuthControlledPortStatus -- authorized*
  - *AuthControlledPortControl -- ForceAuthorized*
- Configure default port VLAN on right side of switch to VLAN 10
  - This includes ports for NAA, RADIUS Simulator, and DHCP server on 192.168.1.1
- Configure default port VLAN on left side of switch to VLAN 20
  - This includes port for DHCP server on 192.168.2.1

4.1.2 Validate Common Setup

Before running any tests, validate the test environment as follows:

Test Steps:

Validate network forwarding:

1. Disconnect Access Requestor from PEP if connected
   a. Maintain disconnect state for at least 10 seconds
2. Set port VLAN-ID to 10
3. Manually disable port access control (802.1X) for Access Requestor
   Particular technique may vary based on individual PEP. The MIB settings that are

expected to be observed (using a MIB browser) are:
   a. *AuthControlledPortStatus -- authorized*
   b. *AuthControlledPortControl -- ForceAuthorized*

4. Begin capturing traffic with both Network Analyzer 1 and 2.
5. Connect Access Requestor
6. Verify Access Requestor IP address on 192.168.1.x/24
7. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1 and the DHCP server at 192.168.2.1.
8. Stop capturing traffic, and verify that traffic from the Access Requestor is permitted and shows up on Network Analyzer 1 and not on Network Analyzer 2.
9. Disconnect Access Requestor from PEP
   a. Maintain disconnect state for at least 10 seconds
10. Set port VLAN-ID to 20
11. Begin capturing traffic with both Network Analyzer 1 and 2.
12. Reconnect Access Requestor to PEP
13. Verify Access Requestor IP address on 192.168.2.x/24
14. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1 and the DHCP server at 192.168.2.1.
15. Stop capturing traffic, and verify that traffic from the Access Requestor is permitted and shows up on Network Analyzer 2, but not on Network Analyzer 1.

Validate authentication-based network forwarding - NAA

1. Configure PEP to use NAA as its RADIUS server.
2. Configure NAA to send an Access-Accept upon successful authentication.
3. Disconnect Access Requestor from PEP (if connected)
   a. Maintain disconnect state for at least 10 seconds
4. Set port VLAN-ID to 10
5. Enable port access control (802.1X) to authenticate Access Requestor.
   Particular technique may vary based on individual PEP techniques, here are the expected MIB settings that are expected to be observed (using a MIB browser)
   a. *AuthControlledPortStatus -- unauthorized*
   b. *AuthControlledPortControl -- Auto*
6. Begin capturing traffic with both Traffic Analyzer 1 and 2.
7. Connect Access Requestor
8. Authenticate Access Requestor to network through the PEP.
9. Verify Access Requestor IP address on 192.168.1.x/24
10. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1 and the DHCP server at 192.168.2.1.
11. Verify that traffic from the Access Requestor is permitted and shows up on Network Analyzer 1 and not on Network Analyzer 2.
12. Verify that RADIUS traffic between PEP and NAA appears on Network Analyzer 1

Validate authentication-based network forwarding - RADIUS Simulator

1. Configure PEP to use RADIUS Simulator as its RADIUS server.

2. Configure RADIUS Simulator to send an Access-Accept upon successful authentication.
3. Disconnect Access Requestor from PEP (if connected)
    b. Maintain disconnect state for at least 10 seconds
4. Set port VLAN-ID to 10
5. Enable port access control (802.1X) to authenticate Access Requestor.
   Particular technique may vary based on individual PEP techniques, here are the expected MIB settings that are expected to be observed (using a MIB browser)
    c. *AuthControlledPortStatus -- unauthorized*
    d. *AuthControlledPortControl -- Auto*
6. Begin capturing traffic with both Traffic Analyzer 1 and 2.
7. Connect Access Requestor
8. Authenticate Access Requestor to network through the PEP.
9. Verify Access Requestor IP address on 192.168.1.x/24
10. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1 and the DHCP server at 192.168.2.1.
11. Verify that traffic from the Access Requestor is permitted and shows up on Network Analyzer 1 and not on Network Analyzer 2.
12. Verify that RADIUS traffic between PEP and RADIUS Simulator appears on Network Analyzer 1

Expected Outcomes:

- Network traffic flows as expected.
- Access Requestor successfully authenticates against both NAA and RADIUS Simulator.
- Traffic destined for each DHCP server is permitted or denied as expected.

5 Test Cases

In test cases where there are multiple expected outcomes listed, all of the expected outcomes must be met in order to pass the test. In test cases where there are multiple anticipated failures listed, any single failure results in failing the test.

5.1 IF-PEP Compliance Test Cases for PEPs

In the IF-PEP Compliance Test Cases for PEPs, the Device Under Test (DUT) is the PEP. To verify that the PEP correctly implements the authentication handshake, the test program will examine the authentication and test traffic generated by the Access Requestor and captured by Network Analyzer 1.

NOTE: Requirement [CTNC-IFPEP1.0-NAA-REQ-1] says that all PEPs MUST support at least one of the following three isolation techniques: binary isolation, VLAN-based isolation, or filter-based isolation. In practice, all NAAs and PEPs support binary isolation, and many support VLAN-based or filter-based isolation. The test administrator should consult with the PEP manufacturer to determine which of these isolation techniques are implemented in the PEP and then run every test case for which the isolation technique is implemented. If the PEP does not implement binary isolation, then this test suite cannot be run.

5.1.1 Binary Isolation and Basic Authentication Functions

[CTNC-IFPEP1.0-PEP-TC-1]

Purpose: To verify that the PEP supports binary isolation, uses a Code field value equal to 1 (Access-Request packet) in all RADIUS messages that it sends during an authentication exchange, includes either a NAS-IP-Address attribute or a NAS-Identifier attribute (or both) in all Access-Request messages that it sends, and sends valid Identifier and Request Authenticator field values and Message-Authenticator attributes. This test case is for the following requirements: [CTNC-IFPEP1.0-PEP-REQ-1-M], [CTNC-IFPEP1.0-PEP-REQ-7-M], [CTNC-IFPEP1.0-PEP-REQ-13-M], [CTNC-IFPEP1.0-PEP-REQ-14-M], [CTNC-IFPEP1.0-PEP-REQ-16-M], [CTNC-IFPEP1.0-PEP-REQ-18-M], [CTNC-IFPEP1.0-PEP-REQ-23-M], [CTNC-IFPEP1.0-PEP-REQ-24-M], [CTNC-IFPEP1.0-PEP-REQ-25-M], [CTNC-IFPEP1.0-PEP-REQ-32-M], and [CTNC-IFPEP1.0-PEP-REQ-34-M].

Preconditions: Devices configured to "*Common Setup"* . NAA configured to send a Class attribute in the Access-Accept.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to NAA through PEP.
3. Ping the DHCP Server at 192.168.1.1 from the Access Requestor.
4. Stop capturing traffic with Network Analyzer 1.
5. Verify that ping traffic from the Access Requestor to the DHCP Server at 192.168.1.1 was captured by Network Analyzer 1.
6. By analyzing traffic captured by Network Analyzer 1, verify that the following conditions apply:
   a) Verify that the Code field value is equal to 1 for all RADIUS packets sent by the PEP during the authentication exchange.
   b) Compare the Identifier field value for all RADIUS packets sent by the PEP during the authentication exchange. Verify that the Identifier field value changes whenever the contents of the Attributes field changes and whenever a valid reply has been

received for a previous request. Further, verify that the Identifier field value is unchanged for retransmissions (if any).

c) Ensure that the Request Authenticator field value in each RADIUS packet sent by the PEP changes each time a new Identifier is used.

d) Verify that all Access-Request messages sent by the PEP during the authentication exchange include either a NAS-IP-Address attribute or a NAS-Identifier attribute or both.

e) Verify that all Access-Request messages sent by the PEP during the authentication exchange include a User-Name attribute.

f) Verify that any Text or String attributes sent by the PEP during the authentication exchange (such as User-Name) do not have a text length of 0 (attribute Length field equal to 2).

g) Verify that the Message-Authenticator sent from the PEP to the NAA was valid by doing a hash of the Access-Accept using the shared secret (as specified in section 3.2 of RFC 3579).

h) Verify that the PEP did not violate the attribute transmission requirements contained in section 5.44 of RFC 2865.Disconnect Access Requestor from PEP.

7. Begin capturing traffic with Network Analyzer 1.
8. Disconnect the Access Requestor, wait 10 seconds, and unsuccessfully authenticate Access Requestor.
9. Attempt to ping the DHCP Server at 192.168.1.1 from the Access Requestor.
10. Stop capturing traffic with Network Analyzer 1.
11. Verify that NO traffic from the Access Requestor is captured by Network Analyzer 1.

Expected Outcomes:

- When the Access Requestor has successfully authenticated, traffic from the Access Requestor is delivered to DHCP Server 1.
- When the Access Requestor has not successfully authenticated, traffic from the Access Requestor is NOT delivered to DHCP Server 1.
- All of the conditions listed in test step 6 apply.

Anticipated Failures:

- When the Access Requestor has successfully authenticated, traffic from Access Requestor is not captured by Network Analyzer 1.
- When the Access Requestor has not successfully authenticated, traffic from the Access Requestor is captured by Network Analyzer 1.
- One of the conditions listed in test step 6 is not met.

5.1.2 VLAN-Based Isolation (Success)

[CTNC-IFPEP1.0-PEP-TC-2]

Purpose: To verify that if the PEP supports VLAN-based isolation, it adheres to RFC2868 tunnel attributes section 3.1 and 3.2, and 3.6 and RFC3580 section 3.31 usage guidelines. This test case only applies if the PEP supports VLAN-based isolation.

This test case is for the following requirement: [CTNC-IFPEP1.0-PEP-REQ-3-M], [CTNC-IFPEP1.0-PEP-REQ-36-M], and [CTNC-IFPEP1.0-PEP-REQ-38-M].

Pre-conditions: Devices configured to "*Common Setup*". Additionally:

- Configure NAA to inform PEP to enforce VLAN-based isolation using the following set of attributes:
    - Tunnel-type (set to a value 13 for "VLAN"),
    - Tunnel-Medium-Type (set to a value of 6 for "802")
    - Tunnel-Private-Group-ID attributes (set to the string "10" to refer to VLAN 10)

The Tag field should set to 0 for both the Tunnel-Type and Tunnel-Medium-Type attributes.

***Test Steps**:*

1. Begin capturing traffic with both Network Analyzer 1 and Network Analyzer 2.
2. Authenticate Access Requestor to NAA through PEP.
3. Generate traffic with Access Requestor - attempt to ping both DHCP servers (192.168.2.1 and 192.168.1.1).
4. By analyzing traffic captured by Network Analyzer 1 and Network Analyzer 2, verify that traffic from the Access Requestor appears only on VLAN 10.

Expected Outcomes:

- NAA sends the VLAN attributes (Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID) to PEP
- Access Requestor sends ping traffic that appears only on VLAN 10

Anticipated Failures:

- PEP might not support VLAN-based Isolation
    - Traffic appears on VLAN 20
    - Traffic does not appear on VLAN 10
- PEP does not support RFC 3580 section 3.31 requirements, such as:
    - Expects to receive VLANID in Tunnel-Private-Group-ID as a RADIUS integer, not a string
    - Expects to receive Tunnel-Medium-Type value of "802" instead of "6" (the enumerated value representing IEEE 802 tunnel types)
    - PEP does not respond to Tunnel-Private-Group-ID attribute Tag field set to 0, but may respond to Tag field set to 01 or Tag field not present

5.1.3 VLAN-Based Isolation (Failure)

[CTNC-IFPEP1.0-PEP-TC-3]

Purpose: To verify that if the PEP supports VLAN-based isolation, it adheres to RFC2868 tunnel attributes section 3.1, 3.2, and 3.6 and RFC3580 section 3.31 usage guidelines, specifically, the requirement that unknown Tunnel-Type and Tunnel-Medium-Types are treated as rejection messages by the PEP. This test case only applies if the PEP supports VLAN-based isolation.

This test case is for the following requirements: [CTNC-IFPEP1.0-PEP-REQ-3-M], [CTNC-IFPEP1.0-PEP-REQ-35-M], and [CTNC-IFPEP1.0-PEP-REQ-37-M].

Preconditions: Devices configured to "*Common Setup*". Additionally:

- Configure NAA to inform PEP to enforce VLAN-based isolation using the following set of attributes:

- Tunnel-type (set to the invalid value of 0xFFFFFF)
- Tunnel-Medium-Type (set to a value of 6 for "802") and
- Tunnel-Private-Group-ID (set to "10" for the internal VLAN).

The Tag field should set to 0 for both the Tunnel-Type and Tunnel-Medium-Type attributes.

Test Steps*:*

1. Begin capturing traffic with both Network Analyzer 1 and Network Analyzer 2.
2. Authenticate Access Requestor to NAA through PEP.
3. Generate traffic with Access Requestor - ping both DHCP servers (192.168.2.1 and 192.168.1.1.
4. By analyzing traffic captured by Network Analyzer 1 and Network Analyzer 2, verify that traffic from Access Requestor is not seen on either VLAN 10 or VLAN 20.
5. Change the configuration of the NAA to inform PEP to enforce VLAN-based isolation using the following set of attributes:
    a. Tunnel-type (set to a value 13 for "VLAN")
    b. Tunnel-Medium-Type (set to the invalid value of 0xFFFFFF) and
    c. Tunnel-Private-Group-ID (set to "10" for the internal VLAN).
    d. The Tag field should set to 0 for both the Tunnel-Type and Tunnel-Medium-Type attributes.
6. Authenticate Access Requestor to NAA through PEP.
7. Generate traffic with Access Requestor - ping both DHCP servers (192.168.2.1 and 192.168.1.1.
8. By analyzing traffic captured by Network Analyzer 1 and Network Analyzer 2, verify that traffic from Access Requestor is not seen on either VLAN 10 or VLAN 20.

Expected Outcomes:

- NAA sends the VLAN attributes (Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID) to PEP
- In both steps 4 & 8, the attempt to connect to the network by Access Requestor is rejected, and no client traffic is seen by either network analyzer.

Anticipated Failures:

- PEP might not support VLAN-based Isolation
- PEP does not support RFC 2868 requirements to treat unknown values of Tunnel-Type and Tunnel-Medium type as reject messages and therefore passes traffic.
- Traffic sent by the Access Requestor is seen on VLAN 10 or VLAN 20.

5.1.4 Filter-Based Isolation

[CTNC-IFPEP1.0-PEP-TC-4]

Purpose: To verify that if the PEP supports Filter-based isolation, it supports the Filter-ID attribute as defined in RFC 2865. This test case only applies if the PEP supports filter-based isolation.

This test case is for the following requirements: [CTNC-IFPEP1.0-PEP-REQ-4-M] and [CTNC-IFPEP1.0-PEP-REQ-26-M] .

Preconditions: Devices configured to "*Common Setup*"**.** Additionally:

- Configure PEP in an unspecified manner with a filter that blocks access to the NAA at 192.168.1.20 and allows access to the DHCP server at 192.168.1.1.
- Configure NAA to inform PEP to enforce filter-based isolation using following attribute:
  - Filter-ID (set to name of the filter defined in the preconditions)

Test Steps*:*

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to NAA through PEP.
3. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1 and the NAA at 192.168.1.20.
4. Stop capturing traffic with Network Analyzer 1.
5. By analyzing traffic captured by Network Analyzer 1, verify that traffic from the Access Requestor appears on VLAN 10 only going to the DHCP server at 192.168.1.1.

Expected Outcomes:

- NAA sends the Filter attribute to PEP.
- Client sends ping traffic to both the NAA 192.168.1.20 and DHCP server 192.168.1.1.
- Traffic destined for the DHCP server 192.168.1.1 is permitted.
- Traffic destined for the NAA on 192.168.1.20 is not permitted.

Anticipated Failures:

- Traffic destined for the NAA 192.168.1.20 is permitted.
- Traffic destined for the DHCP server 192.168.1.1 is not permitted.

5.1.5 Successful CoA with VLANs

[CTNC-IFPEP1.0-PEP-TC-5]

Purpose: To verify that if the PEP supports dynamic policy changes (as described in section 5.4 of IF-PEP), it supports CoA as described in RFC3576. This test case only applies if the PEP supports VLAN-based isolation and dynamic policy changes.

This test case is for the following requirements: [CTNC-IFPEP1.0-PEP-REQ-5-M], [CTNC-IFPEP1.0-PEP-REQ-46-M], [CTNC-IFPEP1.0-PEP-REQ-47-M], and [CTNC-IFPEP1.0-PEP-REQ-48-M].

Preconditions: Devices configured to "*Common Setup*". Additionally:

- Configure NAA to place compliant endpoints on VLAN 10 and non-compliant endpoints on VLAN 20.
- Ensure that endpoint is compliant with NAA policy.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to NAA through PEP. Access Requestor should be placed on VLAN 10.
3. Verify that Access Requestor is on VLAN 10 by pinging DHCP servers 192.168.2.1 and 192.168.1.1. Responses should only be received from DHCP server 192.168.1.1. If this is not true, configuration or operation is incorrect.

4. Change the compliance policy on the NAA so that the NAA concludes that the Access Requestor no longer complies and therefore needs to be placed on VLAN 20.
    a. NAA sends a CoA-Request to PEP.
    b. PEP should respond with a CoA-ACK.
5. Check whether the Access Requestor has an IP address from 192.168.2.0 to 192.168.2.255. If not, force a manual DHCP release and renew.
6. Verify that Access Requestor is on VLAN 20 by pinging DHCP servers 192.168.2.1 and 192.168.1.1. Responses should only be received from DHCP server 192.168.2.1. If this is not true, configuration or operation is incorrect.
7. Stop capturing traffic with Network Analyzer 1.
8. By analyzing traffic captured by Network Analyzer 1, verify that the value of the State attribute in the CoA-ACK message is the same as the value of the State attribute that was sent in the CoA-Request and that the CoA-ACK does not include Error-Cause values 400-599.

Expected Outcomes

- Prior to the policy change, the Access Requestor is only able to ping DHCP server 192.168.1.1 not DHCP server 192.168.2.1.
- After the policy change, the Access Requestor is only able to ping DHCP server 192.168.2.1 not DHCP server 192.168.1.1.
- The value of the State attribute in the CoA-ACK message is the same as the value of the State attribute in the CoA-Request.
- The CoA-ACK does not include Error-Cause values 400-599.

Anticipated Failures:

- Device might not support Dynamic Policy Updates.
- Device might not support VLAN-based isolation.
- Access Requestor didn’t get moved to VLAN 20 and get an IP address from 192.168.2.0 to 192.168.2.255.
- The value of the State attribute in the CoA-ACK message differs from the value of the State attribute in the CoA-Request.
- The CoA-ACK included an Error-Cause value in the range 400-599.

5.1.6 Successful CoA with Filter-ID

[CTNC-IFPEP1.0-PEP-TC-6]

Purpose: To verify that if the PEP supports dynamic policy changes (as described in section 5.4 of IF-PEP), it supports CoA as described in RFC3576. This test case only applies if the PEP supports filter-based isolation and dynamic policy changes.

This test case is for the following requirements: [CTNC-IFPEP1.0-PEP-REQ-5-M], [CTNC-IFPEP1.0-PEP-REQ-46-M], [CTNC-IFPEP1.0-PEP-REQ-47-M], and [CTNC-IFPEP1.0-PEP-REQ-48-M].

Preconditions: Devices configured to “*Common Setup”*. Additionally:

- Configure the PEP in an unspecified manner with two filters:
    - One named “DHCP-only” that blocks access to the NAA at 192.168.1.20 and allows access to the DHCP server at 192.168.1.1 and

  - One named “all” that allows access to both the NAA at 192.168.1.20 and the DHCP server at 192.168.1.1.
- Configure the NAA so that compliant endpoints get the “all” filter-ID assigned and non-compliant endpoints get the “DHCP-only” filter assigned.
- Ensure that endpoint is compliant with NAA policy.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to NAA through PEP.
   a. Access Requestor should receive filter ID “all”.
3. Verify that the Access Requestor received filter ID “all” by pinging DHCP server 192.168.1.1 and NAA 192.168.1.20. Responses should be received from both. If this is not true, configuration or operation is incorrect.
4. Change the compliance policy on the NAA so that the NAA concludes that the Access Requestor no longer complies and therefore needs to have filter ID “DHCP-only” applied.
   a. NAA sends a CoA-Request to PEP.
   b. PEP should respond with a CoA-ACK.
5. Verify that Access Requestor received filter ID “DHCP-only” by pinging DHCP server 192.168.1.1 and NAA 192.168.1.20. Responses should be received from DHCP server 192.168.1.1 but not NAA 192.168.1.20.
6. Stop capturing traffic with Network Analyzer 1.
7. By analyzing traffic captured by Network Analyzer 1, verify that the value of the State attribute in the CoA-ACK message is the same as the value of the State attribute that was sent in the CoA-Request and that the CoA-ACK does not include Error-Cause values 400-599.

Expected Outcomes

- Prior to the policy change, the Access Requestor should be able to ping DHCP server 192.168.1.1 and NAA 192.168.1.20.
- After the policy change, the Access Requestor should only be able to ping DHCP server 192.168.1.1.
- The value of the State attribute in the CoA-ACK message is the same as the value of the State attribute in the CoA-Request.
- The CoA-ACK does not include Error-Cause values 400-599.

Anticipated Failures:

- Device might not support Dynamic Policy Updates.
- Device might not support filter-based isolation.
- Access Requestor didn’t get filter ID “DHCP-only” applied, so it could still ping the NAA.
- The value of the State attribute in the CoA-ACK message differs from the value of the State attribute in the CoA-Request.
- The CoA-ACK included an Error-Cause value in the range 400-599.

5.1.7 Successful Disconnect

[CTNC-IFPEP1.0-PEP-TC-7]

Purpose: To verify that if the PEP supports dynamic policy changes (as described in section 5.4 of IF-PEP), it supports Disconnect as described in RFC3576. This test case only applies if the PEP supports binary isolation and dynamic policy changes.

This test case is for the following requirements: [CTNC-IFPEP1.0-PEP-REQ-5-M], [CTNC-IFPEP1.0-PEP-REQ-46-M], [CTNC-IFPEP1.0-PEP-REQ-47-M], and [CTNC-IFPEP1.0-PEP-REQ-48-M].

Preconditions: Devices configured to "*Common Setup"*. Additionally:

- o Configure the NAA so that compliant endpoints get access to DHCP server 192.168.1.1 and NAA 192.168.1.20, but non-compliant endpoints get no network access at all.
- o Ensure that endpoint is compliant with NAA policy.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to NAA through PEP.
    a. Access Requestor should receive network access to DHCP server 192.168.1.1 and NAA 192.168.1.20.
3. Verify that the Access Requestor received network access to DHCP server 192.168.1.1 and NAA 192.168.1.20 by pinging DHCP server 192.168.1.1 and NAA 192.168.1.20. Responses should be received from both. If this is not true, configuration or operation is incorrect.
4. Change the compliance policy on the NAA so that the NAA concludes that the Access Requestor no longer complies and therefore needs to have no network access at all.
    a. NAA sends a Disconnect-Request to PEP.
    b. PEP should respond with a Disconnect-ACK.
5. Verify that Access Requestor received no network access at all by pinging DHCP server 192.168.1.1 and NAA 192.168.1.20. No responses should be received from DHCP server 192.168.1.1 or NAA 192.168.1.20.
6. Stop capturing traffic with Network Analyzer 1.
7. By analyzing traffic captured by Network Analyzer 1, verify that the value of the State attribute in the Disconnect-ACK message is the same as the value of the State attribute that was sent in the Disconnect-Request and that the Disconnect-ACK does not include Error-Cause values 400-599.

Expected Outcomes

- Prior to the policy change, the Access Requestor should be able to ping DHCP server 192.168.1.1 and NAA 192.168.1.20.
- After the policy change, the Access Requestor should not be able to ping DHCP server 192.168.1.1 or NAA 192.168.1.20.
- The PEP sends a Disconnect-ACK.
- The value of the State attribute in the Disconnect-ACK message is the same as the value of the State attribute in the Disconnect-Request.
- The Disconnect-ACK does not include Error-Cause values 400-599.

Anticipated Failures:

- Device might not support Dynamic Policy Updates.
- Access Requestor didn't get disconnected, so it could still ping the DHCP server or NAA.

- The PEP did not send a Disconnect-ACK.
- The value of the State attribute in the Disconnect-ACK message differs from the value of the State attribute in the Disconnect-Request.
- The Disconnect-ACK included an Error-Cause value in the range 400-599.

5.1.8 Non-Obvious RADIUS Secret Support

[CTNC-IFPEP1.0-PEP-TC-8]

Purpose: To verify that the PEP supports usage of non-obvious RADIUS secrets as described in RFC2865.

This test case is for the following requirement: [CTNC-IFPEP1.0-PEP-REQ-6-M].

Preconditions: Devices configured to "*Common Setup".* Additionally:

- Configure NAA and PEP to use a RADIUS secret composed of 16 octets with spaces and punctuation but no high bit characters (values 128-255).
- Configure NAA to send an Access-Accept upon successful authentication.

Test Steps*:*

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to NAA through PEP.
3. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1.
4. Stop capturing traffic with Network Analyzer 1.
5. By analyzing traffic captured by Network Analyzer 1, verify that traffic from the Access Requestor is permitted.

Expected Outcomes:

- NAA and PEP use the non-obvious RADIUS secret.
- Access Requestor successfully authenticates.
- Traffic destined for the DHCP server is permitted.

Anticipated Failures:

- Not permitted to configure a non-obvious RADIUS secret.
- Configuration of a non-obvious RADIUS secret is permitted, but authentication doesn't work
- Traffic destined for the DHCP server is not permitted.

5.1.9 Message-Authenticator Attribute Support (Failure)

[CTNC-IFPEP1.0-PEP-TC-9]

Purpose: To verify that the PEP supports Message-Authenticator attribute as described in RFC3579, section 3.2. The requirement for the PEP to send valid Message-Authenticator attributes is verified in [CTNC-IFPEP1.0-PEP-TC-1]; this test case verifies behavior when the PEP receives an invalid Message-Authenticator attribute,

This test case is for the following requirement: [CTNC-IFPEP1.0-PEP-REQ-7-M].

Preconditions: Devices configured to "*Common Setup"*. Additionally:

- RADIUS Simulator configured to send Access-Accept with invalid Message-Authenticator attribute.
- PEP configured to use the RADIUS Simulator instead of the NAA.

***Test Steps**:*

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to RADIUS Simulator through PEP.
3. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1.
4. By analyzing traffic captured by Network Analyzer 1, verify that traffic from the Access Requestor is not permitted.

Expected Outcomes:

- PEP silently discards Access-Accept packet from RADIUS Simulator with invalid Message-Authenticator attribute.
- Although the Access Requestor successfully authenticates, the Access-Accept message is not accepted by PEP.
- Traffic destined for the DHCP server is not permitted.

Anticipated Failures:

- Traffic is permitted despite the RADIUS Simulator sending an invalid Message-Authenticator attribute.

5.1.10 Unrecognized Service-Type in Access-Accept

[CTNC-IFPEP1.0-PEP-TC-10]

Purpose: To verify that the PEP treats an Access-Accept authorizing an unavailable service as an Access-Reject.

This test case is for the following requirements: [CTNC-IFPEP1.0-PEP-REQ-8-M] and [CTNC-IFPEP1.0-PEP-REQ-9-M].

Preconditions: Devices configured to "*Common Setup*". Additionally:

- RADIUS Simulator configured to send Access-Accept with Service-Type attribute with value 0x0000ffff.
- PEP configured to use the RADIUS Simulator instead of the NAA.

***Test Steps**:*

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to RADIUS Simulator through PEP.
3. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1.
4. By analyzing traffic captured by Network Analyzer 1, verify that traffic from the Access Requestor is not permitted.

Expected Outcomes:

- RADIUS Simulator uses the unrecognized Service-Type attribute value.
- Although the Access Requestor successfully authenticates, the Access-Accept message is treated as an Access-Reject by PEP.
- Traffic from the Access Requestor to the DHCP server is NOT permitted to pass by the PEP and therefore is NOT captured by Network Analyzer 1.

Anticipated Failures:

- The PEP ignores the unrecognized Service-Type attribute value and treats the Access-Accept as an Access-Accept.
- Traffic from the Access Requestor to the DHCP server IS permitted to pass by the PEP and therefore IS captured by Network Analyzer 1.

5.1.11 Access-Request Retransmissions

[CTNC-IFPEP1.0-PEP-TC-11]

Purpose: To verify that the PEP uses the same Request Authenticator, ID, and source port when it is retransmitting an Access-Request packet and the attributes have not changed.

This test case is for the following requirements: [CTNC-IFPEP1.0-PEP-REQ-10-M] and [CTNC-IFPEP1.0-PEP-REQ-17-M].

Preconditions: Devices configured to "*Common Setup"*. Additionally:

- RADIUS Simulator configured to ignore the first Access-Request.
- PEP configured to use the RADIUS Simulator instead of the NAA.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to RADIUS Simulator through PEP.
3. By analyzing traffic captured by Network Analyzer 1, verify retransmitted traffic from the PEP to the RADIUS Simulator.

Expected Outcomes:

- The PEP will send its first Access-Request message to the RADIUS Simulator, but this packet will be ignored.
- The PEP will retransmit the Access-Request packet with the same attributes, Request Authenticator, ID, and source port.
- The PEP will successfully complete the authentication handshake.

Anticipated Failures:

- The PEP will not retransmit the Access-Request packet and therefore not complete the authentication handshake.
- The PEP will retransmit the Access-Request packet with the same attributes but a different Request Authenticator, ID, or source port.

5.1.12 UDP Packet Larger than RADIUS Packet

[CTNC-IFPEP1.0-PEP-TC-12]

Purpose: To verify that the PEP ignores RADIUS attributes beyond the RADIUS packet length.

This test case is for the following requirement: [CTNC-IFPEP1.0-PEP-REQ-11-M].

Preconditions: Devices configured to "*Common Setup"*. Additionally:

- RADIUS Simulator configured to send Access-Accept with the Message-Authenticator attribute contained beyond the RADIUS length
- PEP configured to use the RADIUS Simulator instead of the NAA.

***Test Steps**:*

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to RADIUS Simulator through PEP.
3. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1.
4. By analyzing traffic captured by Network Analyzer 1, verify that traffic from the Access Requestor is not permitted.

Expected Outcomes:

- PEP silently discards Access-Accept packet from RADIUS Simulator with Message-Authenticator attribute because the Message-Authenticator attribute is not within the RADIUS length.
- Although the Access Requestor successfully authenticates, the Access-Accept message is not accepted by PEP.
- Traffic destined for the DHCP server is not permitted.

Anticipated Failures:

- Traffic is permitted despite the RADIUS Simulator sending a Message-Authenticator attribute not contained in the RADIUS length.

5.1.13 Packet Shorter Than Length Field

[CTNC-IFPEP1.0-PEP-TC-13]

***Purpose**:*To verify that the PEP silently discards any RADIUS packet where the packet is shorter than the Length field indicates.

This test case is for the following requirement: [CTNC-IFPEP1.0-PEP-REQ-12-M].

***Preconditions**:* Devices configured to "*Common Setup"*. Additionally:

- RADIUS Simulator configured to send Access-Accept with the Length field set to a value that is greater than the actual length of the packet.
- PEP configured to use the RADIUS Simulator instead of the NAA.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to RADIUS Simulator through PEP.
3. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1.
4. By analyzing traffic captured by Network Analyzer 1, verify that traffic from the Access Requestor is not permitted.

Expected Outcomes:

- PEP silently discards Access-Accept packet from RADIUS Simulator with Message-Authenticator attribute, because the packet is shorter than the Length field indicates
- Although the Access Requestor successfully authenticates, the Access-Accept message is not accepted by PEP.
- Traffic destined for the DHCP server is not permitted.

Anticipated Failures:

- Traffic is permitted despite the RADIUS Simulator sending an Access-Accept packet shorter than the Length field indicates.

5.1.14 Varying Attribute Order

[CTNC-IFPEP1.0-PEP-TC-14]

Purpose: To verify that the PEP successfully completes each authentication handshake regardless of Attribute order and that the PEP correctly implements the post handshake enforcement.

This test case is for the following requirement: [CTNC-IFPEP1.0-PEP-REQ-20-M].

Preconditions: Devices configured to "*Common Setup"*. Additionally:

- RADIUS Simulator configured to send the Challenge with the Message-Authenticator attribute first, and the Access-Accept with the Message-Authenticator last.
- PEP configured to use the RADIUS Simulator instead of the NAA.

Test Steps*:*

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to RADIUS Simulator through PEP.
3. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1.
4. By analyzing traffic captured by Network Analyzer 1, verify that traffic from the Access Requestor is permitted.

Expected Outcomes:

- RADIUS Simulator and PEP use attributes in varying order.
- Access Requestor successfully authenticates.
- Traffic is permitted despite the RADIUS Simulator sending RADIUS attributes in various orders.

Anticipated Failures:

- Traffic destined for the DHCP server is not permitted.

5.1.15 Invalid Attribute Length

[CTNC-IFPEP1.0-PEP-TC-15]

Purpose: To verify that the PEP interprets packets with an invalid attribute length as Access-Reject packets or silently discards them and that the PEP correctly implements the post handshake enforcement.

This test case is for the following requirement: [CTNC-IFPEP1.0-PEP-REQ-21-M].

Preconditions: Devices configured to "*Common Setup"* . Additionally:

- RADIUS Simulator configured to send Access-Accept including a 0-length attribute with attribute ID 200.
- PEP configured to use the RADIUS Simulator instead of the NAA.

Test Steps*:*

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to RADIUS Simulator through PEP.
3. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1.
4. By analyzing traffic captured by Network Analyzer 1, verify that traffic from the Access Requestor is not permitted.

Expected Outcomes:

- PEP silently discards Access-Accept packet from RADIUS Simulator with invalid attribute length
- Access-Accept message is not accepted by PEP.
- Traffic destined for the DHCP server is not permitted.

Anticipated Failures:

- Traffic is permitted despite the RADIUS Simulator sending an attribute with an invalid length.

5.1.16 State Attribute Value

[CTNC-IFPEP1.0-PEP-TC-16]

Purpose: To verify that the PEP includes a State attribute value identical (including null) to the State attribute originally transmitted by the RADIUS Simulator and that the PEP correctly implements the post handshake enforcement.

This test case is for the following requirements: [CTNC-IFPEP1.0-PEP-REQ-22-M] and [CTNC-IFPEP1.0-PEP-REQ-30-M].

Preconditions: Devices configured to "*Common Setup"*. Additionally:

- RADIUS Simulator configured to send, in one Access-Challenge, a State attribute terminated by a NUL (0), and in another Access-Challenge, a State attribute containing an embedded NUL (0).
- PEP configured to use the RADIUS Simulator instead of the NAA.

Test Steps*:*

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to RADIUS Simulator through PEP.
3. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1.
4. By analyzing traffic captured by Network Analyzer 1, verify that traffic from the Access Requestor is permitted.

Expected Outcomes:

- The PEP always includes in its Access-Request a copy of the State attribute sent by the RADIUS server in the preceding Access-Challenge.
- Access Requestor successfully authenticates.
- Traffic destined for the DHCP server is permitted.

Anticipated Failures:

- The PEP echoes back a State attribute in the subsequent Access-Request that is different from State sent in the Access-Challenge.
- If not implemented correctly, the PEP may chop the value of the State at the first NUL.
- Traffic destined for the DHCP server is not permitted.

5.1.17 Post Handshake Enforcement with Framed-Route Attribute

[CTNC-IFPEP1.0-PEP-TC-17]

Purpose: To verify that the PEP handles the Framed-Route attribute without affecting the operation of the protocol and correctly implements the post handshake enforcement.

This test case is for the following requirement: [CTNC-IFPEP1.0-PEP-REQ-31-M].

Preconditions: Devices configured to "*Common Setup*". Additionally:

- RADIUS Simulator configured to send an Access-Accept packet containing one Framed-Route attribute containing a Text field value equal to "192.168.3.0/24 192.168.1.1 1".
- PEP configured to use the RADIUS Simulator instead of the NAA.

Test Steps*:*

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to RADIUS Simulator through PEP.
3. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1.
4. By analyzing traffic captured by Network Analyzer 1, verify that traffic from the Access Requestor is permitted.

Expected Outcomes:

- RADIUS Simulator and PEP use the Framed-Route attribute.
- Access Requestor successfully authenticates.
- Traffic is permitted despite the RADIUS Simulator including the Framed-Route attribute.

Anticipated Failures:

- Traffic destined for the DHCP server is not permitted, or packets are not forwarded properly.

5.1.18 Vendor-Specific Attribute

[CTNC-IFPEP1.0-PEP-TC-18]

Purpose: To verify that the PEP ignores a vendor-specific attribute that it doesn't recognize.

This test case is for the following requirement: [CTNC-IFPEP1.0-PEP-REQ-33-M].

Preconditions: Devices configured to "*Common Setup*". Additionally:

- RADIUS Simulator configured to send a Vendor-Specific attribute with Vendor-ID 16777215 in the Access-Accept message.
- PEP configured to use the RADIUS Simulator instead of the NAA.

Test Steps*:*

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to RADIUS Simulator through PEP.
3. Generate traffic with Access Requestor - ping the DHCP server at 192.168.1.1.
4. By analyzing traffic captured by Network Analyzer 1, verify that traffic from the Access Requestor is permitted.

Expected Outcomes:

- RADIUS Simulator and PEP use the Vendor-Specific attribute.
- Access Requestor successfully authenticates.
- Traffic is permitted despite the RADIUS Simulator sending a Vendor-Specific attribute.

Anticipated Failures:

- Traffic destined for the DHCP server is not permitted.

5.1.19 Unsuccessful Disconnect-Requests

[CTNC-IFPEP1.0-PEP-TC-19]

Purpose: To verify that the PEP responds to a variety of incorrect Disconnect-Requests (unsupported Service-Type, unsupported attributes, mismatch in NAS Identification attributes, and mismatch in Session Identification attributes) with Disconnect-NAKs and continues to provide network access. This test case only applies if the PEP supports binary isolation and dynamic policy changes.

This test case is for the following requirements: [CTNC-IFPEP1.0-PEP-REQ-39-M], [CTNC-IFPEP1.0-PEP-REQ-42-M], [CTNC-IFPEP1.0-PEP-REQ-43-M], [CTNC-IFPEP1.0-PEP-REQ-44-M], and [CTNC-IFPEP1.0-PEP-REQ-45-M].

Preconditions*:* Devices configured to "*Common Setup".* Additionally:

- Ensure that endpoint is compliant with NAA policy.
- PEP configured to use the RADIUS Simulator instead of the NAA.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to RADIUS Simulator through PEP.
    a. Access Requestor should receive network access to DHCP server 192.168.1.1 and NAA 192.168.1.20.
3. Verify that the Access Requestor received network access to DHCP server 192.168.1.1 and NAA 192.168.1.20 by pinging DHCP server 192.168.1.1 and NAA 192.168.1.20. Responses should be received from both. If this is not true, configuration or operation is incorrect.
4. RADIUS Simulator sends a Disconnect-Request with correct User-Name and NAS-IP-Address attributes but a Service-Type of 0x0000ffff to the PEP.
5. The PEP should respond with a Disconnect-NAK. This Disconnect-NAK may include an Error-Cause attribute with value 405 decimal since this indicates that the Service-Type is not supported by the PEP.
6. Verify that Access Requestor still has network access by pinging DHCP server 192.168.1.1 and NAA 192.168.1.20. Responses should be received from DHCP server 192.168.1.1 or NAA 192.168.1.20.
7. RADIUS Simulator sends a Disconnect-Request with correct User-Name and NAS-IP-Address attributes but a vendor-specific attribute with Vendor ID=0xffffff to the PEP.
8. The PEP should respond with a Disconnect-NAK. This Disconnect-NAK may include an Error-Cause attribute with value 401 decimal since this indicates that the Disconnect-Request includes an attribute whose type is not recognized by the PEP.
9. Verify that Access Requestor still has network access by pinging DHCP server 192.168.1.1 and NAA 192.168.1.20. Responses should be received from DHCP server 192.168.1.1 or NAA 192.168.1.20.
10. RADIUS Simulator sends a Disconnect-Request with correct User-Name but an incorrect NAS-IP-Address attribute.

11. The PEP should respond with a Disconnect-NAK. This Disconnect-NAK may include an Error-Cause attribute with value 403 decimal since this indicates that the NAS Identification attributes do not match.
12. Verify that Access Requestor still has network access by pinging DHCP server 192.168.1.1 and NAA 192.168.1.20. Responses should be received from DHCP server 192.168.1.1 or NAA 192.168.1.20.
13. RADIUS Simulator sends a Disconnect-Request with correct NAS-IP-Address but an incorrect User-Name attribute.
14. The PEP should respond with a Disconnect-NAK. This Disconnect-NAK may include an Error-Cause attribute with value 503 decimal since this indicates that the Session Identification attributes do not match.
15. Verify that Access Requestor still has network access by pinging DHCP server 192.168.1.1 and NAA 192.168.1.20. Responses should be received from DHCP server 192.168.1.1 or NAA 192.168.1.20.
16. RADIUS Simulator sends to the PEP a Disconnect-Request with correct User-Name and NAS-IP-Address attributes but with a shared secret that is not configured on the PEP.
17. The PEP should completely ignore this Disconnect-Request, not responding with a message or changing the Access Requestor's access.
18. Verify that Access Requestor still has network access by pinging DHCP server 192.168.1.1 and NAA 192.168.1.20. Responses should be received from DHCP server 192.168.1.1 or NAA 192.168.1.20.
19. Stop capturing traffic with Network Analyzer 1.
20. By analyzing traffic captured by Network Analyzer 1, verify that the value of the State attribute in the Disconnect-NAK messages is the same as the value of the State attribute that was sent in the preceding Disconnect-Request and that the Disconnect-NAKs do not include Error-Cause values 200-299.

Expected Outcomes:

- PEP will send Disconnect-NAKs where specified in the test steps.
- Prior to and after the Disconnect-Requests and Disconnect-NAKs are sent, the Access Requestor should be able to ping DHCP server 192.168.1.1 and NAA 192.168.1.20.
- The value of the State attribute in each Disconnect-NAK message is the same as the value of the State attribute in the preceding Disconnect-Request.
- The Disconnect-NAKs do not include Error-Cause values 200-299.
- The PEP completely ignores a Disconnect-Request that does not use a shared secret configured on the PEP.

Anticipated Failures:

- PEP sends a Disconnect-ACK at any time during this test
- The value of the State attribute in some Disconnect-NAK message is not the same as the value of the State attribute in the preceding Disconnect-Request.
- PEP sends a Disconnect-NAK including an Error-Cause with a value in the range 200-299.
- The PEP does not ignore a Disconnect-Request that does not use a shared secret configured on the PEP.

5.1.20 Unsuccessful CoA-Requests with VLANs

[CTNC-IFPEP1.0-PEP-TC-20]

Purpose: To verify that a PEP that supports VLAN-based isolation responds to a variety of incorrect CoA-Requests (unsupported Service-Type, unsupported attributes, mismatch in NAS Identification attributes, and mismatch in Session Identification attributes) with CoA-NAKs and continues to provide network access as previously directed. This test case only applies if the PEP supports VLAN-based isolation and dynamic policy changes.

This test case is for the following requirements: [CTNC-IFPEP1.0-PEP-REQ-40-M], [CTNC-IFPEP1.0-PEP-REQ-41-M], [CTNC-IFPEP1.0-PEP-REQ-43-M], [CTNC-IFPEP1.0-PEP-REQ-44-M], [CTNC-IFPEP1.0-PEP-REQ-45-M], [CTNC-IFPEP1.0-PEP-REQ-48-M], and [CTNC-IFPEP1.0-PEP-REQ-49-M].

Preconditions*:* Devices configured to "*Common Setup".* Additionally:

- RADIUS Simulator configured to place compliant endpoints on VLAN 10 and non-compliant endpoints on VLAN 20.
- Ensure that endpoint is compliant with NAA policy.
- PEP configured to use the RADIUS Simulator instead of the NAA.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor through RADIUS Simulator to PEP.
   a. Access Requestor should be placed on VLAN 10.
3. Verify that Access Requestor is on VLAN 10 by pinging DHCP servers 192.168.2.1 and 192.168.1.1. Responses should only be received from DHCP server 192.168.1.1. If this is not true, configuration or operation is incorrect.
4. RADIUS Simulator sends to the PEP a CoA-Request with correct User-Name and NAS-IP-Address attributes and correct Tunnel attributes to change the endpoint to VLAN 20 but a Service-Type of 0x0000ffff.
5. The PEP should respond with a CoA-NAK. This CoA-NAK may include an Error-Cause attribute with value 405 decimal since this indicates that the Service-Type is not supported by the PEP.
6. Verify that Access Requestor still has access to VLAN 10 by pinging DHCP server 192.168.1.1, which should respond.
7. RADIUS Simulator sends to the PEP a CoA-Request with correct User-Name and NAS-IP-Address attributes and correct Tunnel attributes to change the endpoint to VLAN 20 but also a vendor-specific attribute with Vendor ID=0xffffff.
8. The PEP should respond with a CoA-NAK. This CoA-NAK may include an Error-Cause attribute with value 401 decimal since this indicates that the CoA-Request includes an attribute whose type is not recognized by the PEP.
9. Verify that Access Requestor still has access to VLAN 10 by pinging DHCP server 192.168.1.1, which should respond.
10. RADIUS Simulator sends to the PEP a CoA-Request with a correct User-Name attribute and correct Tunnel attributes to change the endpoint to VLAN 20 but an incorrect NAS-IP-Address attribute.
11. The PEP should respond with a CoA-NAK. This CoA-NAK may include an Error-Cause attribute with value 403 decimal since this indicates that the NAS Identification attributes do not match.

12. Verify that Access Requestor still has access to VLAN 10 by pinging DHCP server 192.168.1.1, which should respond.
13. RADIUS Simulator sends to the PEP a CoA-Request with a correct NAS-IP-Address attribute and correct Tunnel attributes to change the endpoint to VLAN 20 but an incorrect User-Name attribute.
14. The PEP should respond with a CoA-NAK. This CoA-NAK may include an Error-Cause attribute with value 503 decimal since this indicates that the Session Identification attributes do not match.
15. Verify that Access Requestor still has access to VLAN 10 by pinging DHCP server 192.168.1.1, which should respond.
16. RADIUS Simulator sends to the PEP a CoA-Request with correct User-Name and NAS-IP-Address attributes and correct Tunnel attributes to change the endpoint to VLAN 20 but with a shared secret that is not configured on the PEP.
17. The PEP should completely ignore this CoA-Request, not responding with a message or changing the Access Requestor's access.
18. Verify that Access Requestor still has access to VLAN 10 by pinging DHCP server 192.168.1.1, which should respond.
19. Stop capturing traffic with Network Analyzer 1.
20. By analyzing traffic captured by Network Analyzer 1, verify that the value of the State attribute in the CoA-NAK messages is the same as the value of the State attribute that was sent in the preceding CoA-Request and that the CoA-NAKs do not include Error-Cause values 200-299. Furthermore, verify that the PEP did not respond to the CoA-Request which did not have a shared secret recognized by the PEP.

Expected Outcomes:

- PEP will send CoA-NAKs where specified in the test steps.
- Prior to and after the CoA-Requests and CoA-NAKs are sent, the Access Requestor should be able to ping DHCP server 192.168.1.1.
- The value of the State attribute in each CoA-NAK message is the same as the value of the State attribute in the preceding CoA-Request.
- The CoA-NAKs do not include Error-Cause values 200-299.
- The PEP completely ignores a CoA-Request that does not use a shared secret configured on the PEP.

Anticipated Failures:

- PEP sends a CoA-ACK at any time during this test
- The value of the State attribute in some CoA-NAK message is not the same as the value of the State attribute in the preceding CoA-Request.
- PEP sends a CoA-NAK including an Error-Cause with a value in the range 200-299.
- The PEP does not ignore the CoA-Request that does not use a shared secret configured on the PEP.

5.1.21 Unsuccessful CoA-Requests with Filter-ID

[CTNC-IFPEP1.0-PEP-TC-21]

Purpose: To verify that a PEP that supports filter-based isolation responds to a variety of incorrect CoA-Requests (unsupported Service-Type, unsupported attributes, mismatch in NAS

Identification attributes, and mismatch in Session Identification attributes) with CoA-NAKs and continues to provide network access as previously directed. This test case only applies if the PEP supports filter-based isolation and dynamic policy changes.

This test case is for the following requirements: [CTNC-IFPEP1.0-PEP-REQ-40-M], [CTNC-IFPEP1.0-PEP-REQ-41-M], [CTNC-IFPEP1.0-PEP-REQ-43-M], [CTNC-IFPEP1.0-PEP-REQ-44-M], [CTNC-IFPEP1.0-PEP-REQ-45-M], [CTNC-IFPEP1.0-PEP-REQ-48-M], and [CTNC-IFPEP1.0-PEP-REQ-49-M].

Preconditions*:* Devices configured to "*Common Setup".* Additionally:

- RADIUS Simulator configured so that compliant endpoints get the "all" filter-ID assigned.
- Ensure that endpoint is compliant with NAA policy.
- PEP configured to use the RADIUS Simulator instead of the NAA.
- PEP is configured in an unspecified manner with two filters:
  - One named "DHCP-only" that blocks access to the NAA at 192.168.1.20 and allows access to the DHCP server at 192.168.1.1.
  - One named "all" that allows access to both the NAA at 192.168.1.20 and the DHCP server at 192.168.1.1.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to RADIUS Simulator through PEP.
   a. Access Requestor should receive filter ID "all".
3. Verify that Access Requestor received filter ID "all" by pinging DHCP server 192.168.1.1 and NAA 192.168.1.20. Responses should be received from both. If this is not true, configuration or operation is incorrect.
4. RADIUS Simulator sends to the PEP a CoA-Request with correct User-Name and NAS-IP-Address attributes and a correct Filter-ID attribute to apply filter ID "DHCP-only" to the endpoint but a Service-Type of 0x0000ffff.
5. The PEP should respond with a CoA-NAK. This CoA-NAK may include an Error-Cause attribute with value 405 decimal since this indicates that the Service-Type is not supported by the PEP.
6. Verify that Access Requestor still has filter "all" by pinging NAA 192.168.1.20, which should respond.
7. RADIUS Simulator sends to the PEP a CoA-Request with correct User-Name and NAS-IP-Address attributes and a correct Filter-ID attribute to apply filter ID "DHCP-only" to the endpoint but also a vendor-specific attribute with Vendor ID=0xffffff.
8. The PEP should respond with a CoA-NAK. This CoA-NAK may include an Error-Cause attribute with value 401 decimal since this indicates that the CoA-Request includes an attribute whose type is not recognized by the PEP.
9. Verify that Access Requestor still has filter "all" by pinging NAA 192.168.1.20, which should respond.
10. RADIUS Simulator sends to the PEP a CoA-Request with a correct User-Name attribute and a correct Filter-ID attribute to apply filter ID "DHCP-only" to the endpoint but an incorrect NAS-IP-Address attribute.
11. The PEP should respond with a CoA-NAK. This CoA-NAK may include an Error-Cause attribute with value 403 decimal since this indicates that the NAS Identification attributes do not match.

12. Verify that Access Requestor still has filter "all" by pinging NAA 192.168.1.20, which should respond.
13. RADIUS Simulator sends to the PEP a CoA-Request with a correct NAS-IP-Address attribute and a correct Filter-ID attribute to apply filter ID "DHCP-only" to the endpoint but an incorrect User-Name attribute.
14. The PEP should respond with a CoA-NAK. This CoA-NAK may include an Error-Cause attribute with value 503 decimal since this indicates that the Session Identification attributes do not match.
15. Verify that Access Requestor still has filter "all" by pinging NAA 192.168.1.20, which should respond.
16. RADIUS Simulator sends to the PEP a CoA-Request with correct User-Name and NAS-IP-Address attributes and a correct Filter-ID attribute to apply filter ID "DHCP-only" to the endpoint but with a shared secret that is not configured on the PEP.
17. The PEP should completely ignore this CoA-Request, not responding with a message or changing the Access Requestor's access.
18. Verify that Access Requestor still has filter "all" by pinging NAA 192.168.1.20, which should respond.
19. Stop capturing traffic with Network Analyzer 1.
20. By analyzing traffic captured by Network Analyzer 1, verify that the value of the State attribute in the CoA-NAK messages is the same as the value of the State attribute that was sent in the preceding CoA-Request and that the CoA-NAKs do not include Error-Cause values 200-299. Furthermore, verify that the PEP did not respond to the CoA-Request which did not have a shared secret recognized by the PEP.

Expected Outcomes:

- PEP will send CoA-NAKs where specified in the test steps.
- Prior to and after the CoA-Requests and CoA-NAKs are sent, the Access Requestor should be able to ping NAA 192.168.1.20.
- The value of the State attribute in each CoA-NAK message is the same as the value of the State attribute in the preceding CoA-Request.
- The CoA-NAKs do not include Error-Cause values 200-299.
- The PEP completely ignores a CoA-Request that does not use a shared secret configured on the PEP.

Anticipated Failures:

- PEP sends a CoA-ACK at any time during this test
- The value of the State attribute in some CoA-NAK message is not the same as the value of the State attribute in the preceding CoA-Request.
- PEP sends a CoA-NAK including an Error-Cause with a value in the range 200-299.
- The PEP does not ignore the CoA-Request that does not use a shared secret configured on the PEP.

5.2 IF-PEP Compliance Test Cases for NAAs

In the IF-PEP Compliance Test Cases for NAAs, the Device Under Test (DUT) is the NAA. To verify that the NAA correctly implements the authentication handshake, the test program will examine the Access-Accept, Access-Challenge and Access-Reject packets transmitted by the NAA and captured by Network Analyzer 1.

NOTE: Requirement [CTNC-IFPEP1.0-NAA-REQ-1] says that all NAAs MUST support at least one of the following three isolation techniques: binary isolation, VLAN-based isolation, or filter-based isolation. In practice, all NAAs and PEPs support binary isolation, and many support VLAN-based or filter-based isolation. The test administrator should consult with the NAA manufacturer to determine which of these isolation techniques are implemented in the NAA and then run every test case for which the isolation technique is implemented. If the NAA does not implement binary isolation, then this test suite cannot be run.

5.2.1 Binary Isolation (Success) and Basic Authentication Functions

[CTNC-IFPEP1.0-NAA-TC-1]

Purpose: To verify that a NAA properly conducts an ordinary EAP exchange ending in an Access-Accept.

This test case is for the following requirements: [CTNC-IFPEP1.0-NAA-REQ-1], [CTNC-IFPEP1.0-NAA-REQ-7], [CTNC-IFPEP1.0-NAA-REQ-13], [CTNC-IFPEP1.0-NAA-REQ-14], [CTNC-IFPEP1.0-NAA-REQ-15], [CTNC-IFPEP1.0-NAA-REQ-17], [CTNC-IFPEP1.0-NAA-REQ-18], [CTNC-IFPEP1.0-NAA-REQ-22], [CTNC-IFPEP1.0-NAA-REQ-23], and [CTNC-IFPEP1.0-NAA-REQ-27]

Preconditions: Devices configured to "*Common Setup".*

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to NAA through PEP.
3. By analyzing traffic captured by Network Analyzer 1, verify that the following conditions apply:
    1. All of the RADIUS packets sent by the NAA during this exchange are Access-Challenge messages except the final message in the exchange, which is an Access-Accept message
    2. The final message sent by the NAA during this exchange (the Access-Accept) does not contain any attributes related to VLAN- or filter-based isolation
    3. RADIUS Access-Accept or Access-Challenge messages from NAA to PEP that contain the EAP-Message attribute contain the Message-Authenticator attribute
    4. The Response Authenticator fields in the packets sent by the NAA contain the correct responses for the pending Access-Requests
    5. No Text or String attributes sent by the NAA are zero length
    6. The attributes sent by the NAA comply with table 5.44 of RFC 2865.

Expected Outcomes:

- All of the conditions listed in test step 3 apply.

Anticipated Failures:

- NAA cannot be configured for binary isolation.
- One of the conditions listed in test step 3 is not met.

5.2.2 Binary Isolation (Failure)

[CTNC-IFPEP1.0-NAA-TC-2]

Purpose: To verify that a NAA properly conducts an ordinary EAP exchange ending in an Access-Reject.

This test case is for the following requirements: [CTNC-IFPEP1.0-NAA-REQ-9], [CTNC-IFPEP1.0-NAA-REQ-13], [CTNC-IFPEP1.0-NAA-REQ-16], and [CTNC-IFPEP1.0-NAA-REQ-17].

Preconditions: Devices configured to *“Common Setup”.*

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Using a Access Requestor that will always fail to authenticate, attempt to authenticate through PEP to NAA.
3. By analyzing traffic captured by Network Analyzer 1, verify that expected RADIUS packets were sent by NAA.

Expected Outcomes:

- All of the RADIUS packets sent by the NAA during this exchange are Access-Challenge messages except the final message in the exchange, which is an Access-Reject message.

Anticipated Failures:

- The NAA sends a RADIUS packet other than an Access-Challenge message before the final message in the exchange, or sends a RADIUS packet other than an Access-Reject as the final message.

5.2.3 VLAN-Based Isolation

[CTNC-IFPEP1.0-NAA-TC-3]

Purpose: To verify that if the NAA supports VLAN-based isolation, it adheres to RFC2868 tunnel attributes sections 3.1, 3.22, & 3.6, and RFC3580 section 3.31 usage guidelines.

This test case is for the following requirements: [CTNC-IFPEP1.0-NAA-REQ-1], [CTNC-IFPEP1.0-NAA-REQ-3], [CTNC-IFPEP1.0-NAA-REQ-28], and [CTNC-IFPEP1.0-NAA-REQ-29].

Preconditions: Devices configured to “*Common Setup”*. Additionally:

- Configure NAA to provision PEP to enforce VLAN-based isolation using valid set of :
  - Tunnel-Type (set to a value 13 for "VLAN")
  - Tunnel-Medium-Type (set to a value of 6 for "802")
  - and Tunnel-Private-Group-ID attributes (set to the string "20" to refer to VLAN 20).

The Tag field should be set to 0 for both the Tunnel-Type and Tunnel-Medium-Type attributes.

Test Steps*:*

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to NAA through PEP.
3. By analyzing traffic captured by Network Analyzer 1, verify that expected attributes were sent by NAA.

Expected Outcomes:

- NAA sends the correct, properly formatted VLAN attributes (Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID, including Tag fields with a 0 value) to PEP.

Anticipated Failures:

- NAA does not support RFC 3580 section 3.31 requirements, such as:
  - Sends VLANID in Tunnel-Private-Group-ID as a RADIUS integer, not a string
  - Sends Tunnel-Medium-Type value of 802 instead of 6 (the enumerated value representing IEEE 802 tunnel types)
  - Sends non-zero Tag fields when these fields are unused.

5.2.4 Filter-Based Isolation

[CTNC-IFPEP1.0-NAA-TC-4]

Purpose*:* To verify that if the NAA supports filter-based isolation, it adheres to RFC2865 filter-id attributes section 5.11, and RFC3580 section 3.9 usage guidelines.

This test case is for the following requirements: [CTNC-IFPEP1.0-NAA-REQ-1] and [CTNC-IFPEP1.0-NAA-REQ-4-M].

Preconditions: Devices configured to "*Common Setup*". Additionally:

- o Configure PEP in an unspecified manner with a filter that blocks access to the NAA at 192.168.1.20 and allows access to the DHCP server at 192.168.1.1.
- o Configure NAA to provision PEP to enforce filter-based isolation using a Filter-ID attribute set to the name of the filter defined on the PEP.

Test Steps*:*

1. Begin capturing traffic with Network Analyzer 1.
2. Authenticate Access Requestor to NAA through PEP.
3. By analyzing traffic captured by Network Analyzer 1, verify that expected Filter-ID attribute was sent by NAA.

Expected Outcomes:

- NAA sends the correct, properly formatted filter-ID attribute to PEP.

Anticipated Failures:

- NAA doesn't send a Filter-ID attribute, or it sends an incorrectly formatted Filter-ID attribute.

5.2.5 Dynamic Access Policy Update

[CTNC-IFPEP1.0-NAA-TC-5]

Purpose: To verify that the NAA can successfully modify the access policy for a given endpoint dynamically.

This test case is for the following requirement: [CTNC-IFPEP1.0-NAA-REQ-2].

Preconditions: Devices configured to "*Common Setup".* Additionally:

- o Configure NAA to grant access to compliant Access Requestors and block access to non-compliant Access Requestors.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Using a non-compliant Access Requestor, authenticate through PEP to NAA.
3. By analyzing traffic captured by Network Analyzer 1, verify that RADIUS response from NAA to PEP passed RADIUS attributes to block access to non-compliant Access Requestor.
4. Remediate Access Requestor so as to bring back into compliancy.
5. Re-authenticate compliant Access Requestor through PEP to NAA.
6. By analyzing traffic captured by Network Analyzer 1, verify that RADIUS response from NAA to PEP passed RADIUS attributes to grant access to compliant Access Requestor.

Expected Outcomes:

- NAA generates RADIUS attributes that block access for non-compliant Access Requestor.
- NAA generates RADIUS attributes that allow access for compliant Access Requestor.

Anticipated Failures:

- NAA fails to generate RADIUS attributes that block access for non-compliant Accesss Requestors.
- NAA fails to generate RADIUS attributes that allow access for compliant Access Requestor.

5.2.6 Dynamic Policy Change

[CTNC-IFPEP1.0-NAA-TC-6]

Purpose: If an NAA supports dynamic access policy change initiated by the NAA, this test case ensures that it complies with RFC 3576. IF-PEP specifies the usage of RFC3576 CoA (Change of Authorization) attributes to accomplish changes in access policy without loss in network connectivity.

This test case is for the following requirement: [CTNC-IFPEP1.0-NAA-REQ-5].

Preconditions*:* Devices configured to "*Common Setup". * Additionally:

- Configure NAA to grant access to compliant Access Requestor and isolate non-compliant Access Requestors.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Using a compliant Access Requestor, authenticate through PEP to NAA.
3. By analyzing traffic captured by Network Analyzer 1, verify that RADIUS response from NAA to PEP passed RADIUS attributes to grant access to compliant Access Requestor.
4. Change NAA configuration so that previously-compliant Access Requestor is now non-compliant.
5. By analyzing traffic captured by Network Analyzer 1, verify that NAA sends the appropriate CoA RADIUS attributes to update PEP with new isolation access policy.

Expected Outcomes:

- NAA is capable of generating a RADIUS CoA attribute to update the access policy of the Access Requestor dynamically without interruption in network connectivity.

Anticipated Failures:

- NAA fails to send CoA attribute .
- NAA causes a full reauthentication, thereby causing PEP to temporarily de-authenticate Access Requestor and Access Requestor to lose network connectivity.

5.2.7 Non-Obvious RADIUS secrets

[CTNC-IFPEP1.0-NAA-TC-7]

Purpose: To verify the NAA supports use of non-obvious RADIUS secrets (at least 16 octets) as described in RFC2865.

This test case is for the following requirement: [CTNC-IFPEP1.0-NAA-REQ-6].

Preconditions: Devices configured to "*Common Setup". Additionally:*

- Configure NAA and PEP to use a RADIUS secret composed of 16 octets with spaces and punctuation but no high bit characters (values 128-255).

Test Steps:

1. Start capturing traffic on Network Analyzer 1.
2. Using compliant Access Requestor, authenticate through PEP to NAA.
3. By analyzing traffic captured by Network Analyzer 1, verify that NAA and PEP have completed a RADIUS exchange ending in an Access-Accept.

Expected Outcomes:

- Successful RADIUS authentication sequence that involves usage of the non-obvious RADIUS secret.

Anticipated Failures:

- Not permitted to configure a non-obvious RADIUS secret.
- RADIUS authentication sequence fails.

5.2.8 No Shared Secret

[CTNC-IFPEP1.0-NAA-TC-8]

Purpose*:* To verify that the NAA silently discards the Access-Request from RADIUS clients for which it does not have a shared secret.

This test case is for the following requirement: [CTNC-IFPEP1.0-NAA-REQ-8].

Preconditions: Devices configured to *"Common Setup"*. Additionally:

- Configure the NAA so that it has no shared secret with the PEP.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1
2. Authenticate Access Requestor to NAA through PEP.
3. By analyzing traffic captured by Network Analyzer 1, verify that NAA did not respond to any of the messages sent by the PEP.

Expected Outcomes:

- NAA silently discards the Access-Request from RADIUS clients for which it does not have a shared secret.

Anticipated Failures:

- NAA responds to PEP RADIUS requests.

5.2.9 UDP Packet Larger than RADIUS Packet

[CTNC-IFPEP1.0-NAA-TC-9]

Purpose*:* To verify that the NAA ignores RADIUS attributes beyond the RADIUS packet length.

This test case is for the following requirement: [CTNC-IFPEP1.0-NAA-REQ-10].

Preconditions*:* Devices configured to "*Common Setup*". Additionally:

- RADIUS Simulator configured to send Access-Request with the Message-Authenticator attribute contained beyond the RADIUS length
- NAA configured to recognize the RADIUS Simulator as a RADIUS Client.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Use RADIUS Simulator to generate an EAP over RADIUS exchange with the NAA.
3. By analyzing traffic captured by Network Analyzer 1, verify that the NAA did not respond to any of the messages sent by the RADIUS Simulator.

Expected Outcomes:

- NAA silently discards Access-Request packet from RADIUS Simulator with Message-Authenticator attribute, because the Message-Authenticator attribute is not within the RADIUS length.

Anticipated Failures:

- NAA responds to the packets sent by the RADIUS Simulator.

5.2.10 Packet Shorter Than Length Field

[CTNC-IFPEP1.0-NAA-TC-10]

Purpose*:*To verify that the NAA silently discards any RADIUS packet where the packet is shorter than the Length field indicates.

This test case is for the following requirement: [CTNC-IFPEP1.0-NAA-REQ-11].

Preconditions*:* Devices configured to "*Common Setup*". Additionally:

- RADIUS Simulator configured to send Access-Request with the Length field set to a value that is greater than the actual length of the packet.
- NAA configured to recognize the RADIUS Simulator as a RADIUS Client.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Use RADIUS Simulator to generate an EAP over RADIUS exchange with the NAA.
3. By analyzing traffic captured by Network Analyzer 1, verify that the NAA did not respond to any of the messages sent by the RADIUS Simulator.

Expected Outcomes:

- The NAA silently discards the packets sent by the RADIUS Simulator, because the packet is shorter than the Length field indicates.

Anticipated Failures:

- The NAA responds to the packets sent by the RADIUS Simulator.

5.2.11 Source IP Determines Shared Secret

[CTNC-IFPEP1.0-NAA-TC-11]

Purpose*:* To verify that the NAA uses the source IP address of the RADIUS UDP packet to decide which shared secret to use.

This test case is for the following requirements: [CTNC-IFPEP1.0-NAA-REQ-12], [CTNC-IFPEP1.0-NAA-REQ-24], and [CTNC-IFPEP1.0-NAA-REQ-26].

Preconditions*:* Devices configured to "*Common Setup".* Additionally:

- o NAA configured to recognize the RADIUS Simulator as a RADIUS Client.
- o NAA and RADIUS Simulator configured with a shared secret, but NAA has this shared secret matched with 192.168.1.22 (an unused IP address) and, if possible, with a NAS-Identifier of "example.com". NAA does not have this shared secret associated with RADIUS Simulator's IP address.
- o RADIUS Simulator configured to send a legitimate authentication request to the NAA that includes a NAS-IP-Address attribute with value 192.168.1.22 and a NAS-Identifier attribute with value "example.com" in all Access-Request messages, and uses the shared secret associated with 192.168.1.22.

*"**Test Steps:***

1. Begin capturing traffic with Network Analyzer 1.
2. Use RADIUS Simulator to generate an EAP over RADIUS exchange with the NAA.
3. By analyzing traffic captured by Network Analyzer 1, verify that the NAA did not respond to any of the messages sent by the RADIUS Simulator.

Expected Outcomes:

- NAA silently discards all traffic sent by the RADIUS Simulator in this test case since it does not have a shared secret with the RADIUS Simulator, as determined by the RADIUS Simulator's source IP address.

Anticipated Failures:

- The NAA responds to the packets sent by the RADIUS Simulator.

5.2.12 Different Attribute Order

[CTNC-IFPEP1.0-NAA-TC-12]

Purpose*:* To verify that the NAA correctly implements the handshake regardless of Attribute order in the transmitted Access-Request packets.

This test case is for the following requirement: [CTNC-IFPEP1.0-NAA-REQ-19]. This test is not an exhaustive test of all possible attribute orderings.

Preconditions: Devices configured to "*Common Setup*". Additionally:

- o RADIUS Simulator configured to send a legitimate authentication request in which the first Access-Request contains the Message-Authenticator attribute first, and a subsequent Access-Request contains the Message-Authenticator last.
- o NAA configured to recognize the RADIUS Simulator as a RADIUS Client.

Test Steps*:*

1. Begin capturing traffic with Network Analyzer 1.
2. Use RADIUS Simulator to generate an EAP over RADIUS exchange with the NAA.
3. By analyzing traffic captured by Network Analyzer 1, verify that the NAA and RADIUS Simulator have completed a RADIUS exchange ending in an Access-Accept.

Expected Outcomes:

- Successful RADIUS authentication sequence despite different attribute order.

Anticipated Failures:

- RADIUS authentication sequence fails.

5.2.13 Invalid Attribute Length

[CTNC-IFPEP1.0-NAA-TC-13]

Purpose*:*To verify that the NAA silently discards any RADIUS packet with an invalid attribute length.

This test case is for the following requirement: [CTNC-IFPEP1.0-NAA-REQ-20].

Preconditions*:* Devices configured to "*Common Setup*". Additionally:

- RADIUS Simulator configured to send Access-Request with including a 0-length attribute with attribute ID 200.
- NAA configured to recognize the RADIUS Simulator as a RADIUS Client.

Test Steps:

1. Begin capturing traffic with Network Analyzer 1.
2. Use RADIUS Simulator to generate an EAP over RADIUS exchange with the NAA.
3. By analyzing traffic captured by Network Analyzer 1, verify that the NAA did not respond to any of the messages sent by the RADIUS Simulator.

Expected Outcomes:

- NAA silently discards the packets sent by the RADIUS Simulator, because the packet contains an attribute with an invalid length.

Anticipated Failures:

- NAA responds to the packets sent by the RADIUS Simulator.

5.2.14 Embedded NUL

[CTNC-IFPEP1.0-NAA-TC-14]

Purpose*:* To verify that the NAA correctly implements the handshake even if there is an embedded NUL in an attribute

This test case is for the following requirement: [CTNC-IFPEP1.0-NAA-REQ-21].

Preconditions: Devices configured to "*Common Setup".* Additionally:

- RADIUS Simulator configured to send a legitimate authentication request in which one Access-Request contains a Proxy-State attribute terminated by a NUL (0), and another Access-Request contains a Proxy-State attribute containing an embedded NUL (0)
- NAA configured to recognize the RADIUS Simulator as a RADIUS Client.

Test Steps:

1. Start capturing traffic on Network Analyzer 1.
2. Use RADIUS Simulator to generate an EAP over RADIUS exchange with the NAA.
3. By analyzing traffic captured by Network Analyzer 1, verify that the NAA and RADIUS Simulator have completed a RADIUS exchange ending in an Access-Accept.

Expected Outcomes:

- Successful RADIUS authentication sequence despite embedded NUL.

Anticipated Failures:

- RADIUS authentication sequence fails.

5.2.15 Vendor-Specific Attribute

[CTNC-IFPEP1.0-NAA-TC-15]

Purpose*:* To verify that the operation of the NAA is not affected by a Vendor-Specific attribute that is not recognized by the NAA.

This test case is for the following requirement: [CTNC-IFPEP1.0-NAA-REQ-25].

Preconditions: Devices configured to "*Common Setup"*. Additionally:

- RADIUS Simulator configured to send a legitimate authentication request that includes a Vendor-Specific attribute with Vendor-ID 16777215 in the Access-Request message.
- NAA configured to recognize the RADIUS Simulator as a RADIUS Client.

Test Steps*:*

1. Begin capturing traffic with Network Analyzer 1.
2. Use RADIUS Simulator to generate an EAP over RADIUS exchange with the NAA.
3. By analyzing traffic captured by Network Analyzer 1, verify that the NAA and RADIUS Simulator have completed a RADIUS exchange ending in an Access-Accept.

Expected Outcomes:

- Successful RADIUS authentication sequence despite presence of vendor-specific attribute.

Anticipated Failures:

- RADIUS authentication sequence fails.

References

This section lists specifications and other documents that are referred to in the document. Since this document is informative (not normative), all of these references are informative with respect to this document.

Informative References

1. Trusted Computing Group, TNC Architecture for Interoperability, Specification Version 1.1, May 2006.

2. Trusted Computing Group, TNC IF-PEP for RADIUS, Specification Version 1.0, May 2006.

3. Trusted Computing Group, Compliance_TNC Compliance and Interoperability Principles, Specification Version 1.0, Draft Specification, October 2006.

4. Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

5. Zorn, G., et al., "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

6. Aboba, B. and P. Calhoun, "RADIUS Support for Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

7. Chiba, M., et. al., "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

8. Congdon, P., et. al., “IETF 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines,” RFC3580, September 2003.