

What is IETF Network Endpoint Assessment?

The Internet Engineering Task Force (IETF) is the ultimate arbiter for Internet protocols. They have standardized dozens of critical protocols like IP, TCP, FTP, HTTP, SMTP, and IPsec. With its many competing and incompatible architectures and standards, Network Access Control is ripe for standardization. Fortunately, the IETF has started a Working Group in this area: the Network Endpoint Assessment (NEA) Working Group.

IETF NEA Goals and Scope

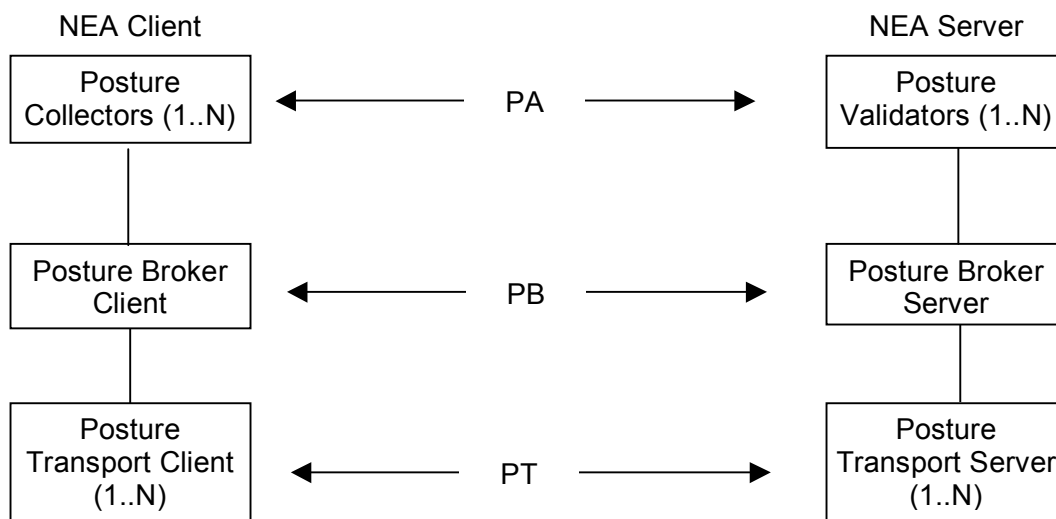
The goal of the IETF NEA Working Group is to agree on and publish certain critical NAC standards. Recognizing that there are already many existing protocols in this area, IETF NEA is starting with a requirements document. Once the requirements document is complete, NEA will solicit candidate protocol specifications, evaluate them against the requirements, and decide whether to approve one of the candidate specs or develop a new one.

The focus of IETF NEA is on client-server protocols. This is appropriate since client-server interoperability has been identified as the highest priority and IETF has generally avoided defining APIs. In order to keep the scope of the IETF NEA effort reasonable, certain topics have been declared explicitly out of scope for IETF NEA: detecting and handling lying endpoints, remediation, enforcement, and non-enterprise deployments. The protocols standardized by IETF NEA may accommodate these areas but IETF NEA will not address them.

IETF NEA Reference Model

In order to have consistent and agreed-upon terminology, IETF NEA has defined the reference model depicted below. This model is similar to existing NAC architectures but it is not intended to favor one architecture over another or to create a new NAC architecture. Rather, it is intended to establish agreement on concepts and terminology for the IETF effort. Thus far, it has been successful in doing so.

The IETF NEA reference model includes two entities: the NEA Client and the NEA Server. Each entity contains several components. On the NEA Client, Posture Collectors gather information about the client's security. A Posture Broker Client gathers information from the Posture Collectors and sends it to the NEA Server over transports provided by one or more Posture Transport Clients. On the NEA Server, a Posture Broker Server receives information about endpoints via one or more Posture Transport Servers and distributes this information to one or more Posture Validators which determine compliance with policy. Enforcement is not addressed in the reference model since it is out of scope for NEA.



IETF NEA Protocols

IETF NEA has identified three protocols as candidates for standardization:

PA – protocol for messages sent between Posture Collectors and Posture Validators

PB – protocol for messages sent from Posture Broker Client to Posture Broker Server

PT – transport protocol

These protocols will be layered (i.e., encapsulated). PA will be carried by PB, which will be transported by PT. This encapsulation should help keep Posture Collectors and Posture Validators simple and allow the NEA protocols to work with a variety of network technologies.

IETF NEA Requirements

The IETF NEA requirements document is still under development and therefore in a state of flux. However, it may be useful to highlight a few of the key requirements here to give a sense of the work under way.

C-1 NEA protocols **MUST** be capable of performing a multiple message dialog between the NEA Client and NEA Server. This allows for assessment models that require more than one round trip to complete the assessment.

C-2 NEA protocols **MUST** allow posture assessment to occur before or after the endpoint has established network connectivity.

C-3 NEA protocols **MUST** provide a way for both the NEA Client and the NEA Server to initiate a posture re-assessment request as needed.

C-4 NEA protocols **MUST** provide protection against active and passive attacks by intermediaries including protection to prevent replay based attacks.

C-6 The selection process for NEA protocols **MUST** evaluate and prefer the reuse of existing open standards that meet the requirements before defining new ones.

PT-4 The PT protocol **MUST** be capable of protecting the integrity and confidentiality of the PB messages between the Posture Transport Client and the Posture Transport Server. This includes protection against replay and reflection.

PT-5 The PT protocol **MUST** provide reliable delivery for the PB protocol. This includes the ability to perform fragmentation, reassembly, and detect duplicates and reorder to provide in-sequence delivery, as required.

PT-6 The PT protocol **MUST** be capable of supporting mutual authentication between the Posture Transport Client and the Posture Transport Server.

IETF NEA Status and Timeline

The IETF NEA Working Group was chartered in October 2006 with a schedule revision in April 2007. It is currently working on requirements and plans to have the requirements document in IETF Last Call by August 2007. The current IETF NEA milestones do not extend beyond that point. New milestones for protocol development will be agreed upon once the requirements document is agreed on. As described in the charter, the first focus of NEA will be the PA and PB protocols. The expectation is that other IETF Working Groups will standardize a PT protocol.

For More Information

As with all IETF Working Groups, all proceedings of the IETF NEA Working Group are available on the IETF web site, <http://www.ietf.org>. This includes draft documents, meeting minutes, and email archives. Most of the work of the IETF NEA Working Group takes place on the nea@ietf.org email list, which is open to anyone who would like to subscribe. For instructions, see the NEA Working Group section of the IETF web page.