

What is the IETF NAC strategy?

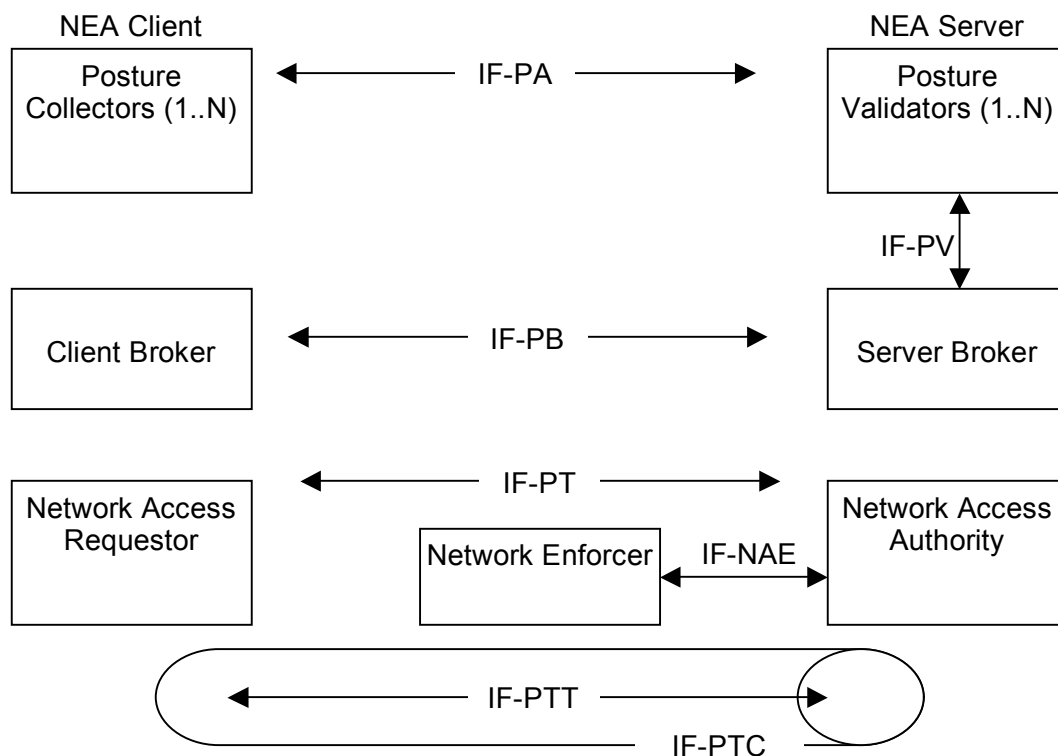
As you may have noticed at the Network Access Control Labs here at Interop Las Vegas 2006, we have three demonstrations showing three different architectures that don't interoperate with each other. Who is going to fix that? Hopefully, the IETF (Internet Engineering Task Force). How soon until they have a solution? We'll get dates for the final solution in summer of 2007 at the earliest. Here is where they are, and where they are focusing.

IETF's Network Endpoint Assessment initiative

The Network Endpoint Assessment (NEA) group of the IETF realizes that companies have already worked to create protocols that work well for them. The IETF's focus now is to add a layer of communication that will allow all of these different pieces to interoperate with each other.

At the IETF meeting in March, 2006, the NEA Birds of a Feather (BOF) group decided what problems they were going to address and what the scope of their work should be. This, along with a new set of names for the components in a NAC architecture, are laid out in a problem statement, published as an Internet draft (available on the IETF's web site for up to 6 months, and archived on the iLabs NAC web site at <http://www.opus1.com/nac/>) called `draft-thomson-nea-problem-statement-01.txt`. This document is very clear in its goal: the definition of protocols that can be used in existing architectures (TCG-TNC, MS-NAP, and C-NAC are all explicitly called out) that will enable better interoperability. In other words, the IETF does not intend to create yet another NAC architecture. Instead, the NEA group aims only to identify common interfaces that are used in these architectures, and define standard protocols that can be used by the existing architectures to reduce duplication and achieve interoperability.

The IETF NEA group identified seven separate interfaces within a NAC architecture (see the diagram below), and specifically called out four of them (IF-PTT, IF-NAE, IF-PB, and IF-PTC) for immediate standardization. The two remaining interfaces, IF-PA and IF-PV, may be addressed at a later date. (IF-PT is just the combination of the IF-PTC and IF-PTT interfaces; in other architectural instantiations, this pair might be defined differently.)



IETF Approach to NAC

The IETF hopes to work on the issues laid out as part of the NEA group's problem statement by either creating new standards to allow these pieces to communicate, or work with other working groups to extend their protocols to handle the data that needs to be communicated. For example, within Internet2, a working group was created called SALSA-NetAuth to solve a similar set of problems. Many of the issues that are being addressed by NEA will also be addressed by SALSA-NetAuth. However, the main goal of the IETF NEA group is to create standards that will allow multiple solutions to interoperate.

Some of the specific areas that the NEA group is concerned about include:

IF-PB: The Posture Broker Interface. This interface defines communication between a client broker and a server broker. These are the technologies that actually collect the postures on the client, and then disassemble them on the server for validation. This protocol also carries the overall system posture result from the server broker to the client broker. Again the IETF admits that this communication doesn't care about the underlying protocols, but specifying this channel, would then simplify the requirements to allow systems to encrypt and transmit this known entity in something like an EAP-TLS tunnel. If it were a proprietary and unknown format, encrypting it and not have a standard on both ends would be more difficult.

IF-PTT: The EAP communication that is used for authentication. The abstract protocol defined in the NEA architecture is **IF-PT** (Posture Transport Interface), which the NEA group broke down into the Posture Transport Tunnel (**IF-PTT**, an EAP tunneling method) and the Posture Transport Carrier (**IF-PTC**, a protocol that carries EAP, such as EAP over 802.1X or EAP over RADIUS). The goal here is to communicate with other working groups to make sure that what the NEA group is proposing can be used over EAP and EAP transports that allow multi-hop deployment scenarios. These working groups are EMU, NACP and PANA.

IF-NAE: The Network Access Enforcement interface. This interface defines the communication from the Network Access Authority to the Network Enforcement Point and the client. Typically this would be RADIUS or DIAMETER. The group is focusing on RADIUS, which would be used in EAP instantiations of this architecture, and is looking specifically to see if any extra RADIUS extensions would be needed for NEA.

IF-PV: The Posture Validation interface. This interface defines the communication between a server broker and a posture validator. In some instantiations of the architecture, the server broker and the posture validators are not co-located. The IF-PV protocol between the server broker and posture validator forwards posture information and returns posture validation results.

IF-PA: The Posture Attribute interface. This interface defines communication between a posture collector (client) and posture validator (server). The interface is used to pass information gathered by a posture collector to the posture validator, and to pass the results of the assessment and information needed for remediation from the posture validator to the posture collector. While it is really only important for a third party server to understand its own third party client, the IETF is looking to create a standard in order to make this communication extensible and usable by other systems.

IETF Standardization Directions

According to the latest problem statement, the first three items (IF-PB, IF-PTT and IF-NAE) are the NEA group's focus. The last two will be addressed as time and importance permit. At the BoF meeting in March 2006, after the first version of the problem statement was drafted, it was clear that the communication between the server broker and the posture validator (the IF-PV interface) is considered important to those that attended. We expect this change to be reflected in the next revision of the problem statement.

The IETF has started the process to bring these three large protocols together, and has invited other smaller innovators to participate as well. The goal is to first determine the requirements, and review what work is already proceeding within the IETF in other working groups that could solve some or all of these requirements. Then, the NEA group will submit proposals for the protocols that would be specifically designed to solve problems that aren't solved elsewhere. By February of 2007, the NEA group will have defined which protocols they wish to create. How long it will take them to create those protocols after they define them is uncertain.