

What is Cisco NAC?

Cisco's Network Admission Control, which we'll call C-NAC to avoid overloading the acronym NAC (for Network Access Control), can be very directly mapped to open standards such as the TCG TNC and proposed IETF architectures. Cisco has published a set of architectural overviews, and this white paper is derived from those overviews as well as the results of our iLabs testing.

When reading this white paper, you may find it helpful to have at hand our companion white paper, "Network Access Control Architecture Alphabet Soup," with the diagram showing the different parts of a NAC architecture.

Client Side (Access Requestor) in C-NAC

On the client side, Cisco's picture maps directly to the proposed IETF architecture. The IETF's Network Access Requestor and the Client Broker are both covered by Cisco's Cisco Trust Agent, a free piece of software. The Posture Collectors appear as vendor-provided agents and as (optionally) Cisco's own Cisco Secure Access, a Host Intrusion Prevention tool. In the iLabs, we are demonstrating LANdesk and InfoExpress Posture Collectors and Validators.

Because Cisco is actually shipping products that support their architecture, they also have gotten serious about the protocols needed to handle Network Admission Control. At the lowest layer, they have selected EAP, the Extensible Authentication Protocol. While EAP was designed by the IETF for authentication and is heavily used in most 802.1X deployments, Cisco has developed their own proprietary EAP method, called EAP-FAST (Flexible Authentication via Secure Tunneling). With EAP-FAST in place, Cisco can include both 802.1X authentication as well as end-point security assessment information in the EAP protocol.

Because Cisco wants their product line to work with more than 802.1X-enabled switches, Cisco's Cisco Trust Agent has both EAP-over-802.1X as well as EAP-over-UDP. The thinking behind this is that when an end-system tries to access the network using a method besides 802.1X, such as a VPN client or even just someone coming in through a non-802.1X switch, the EAP traffic will travel over UDP instead.

There is a serious and critical difference between the 802.1X and UDP versions of Cisco's EAP, though. In the 802.1X case, EAP includes both authentication and end-point security assessment information. When used with UDP, Cisco's NAC no longer does authentication. Instead, the user has to be authenticated via some other mechanism, and the authentication and user credentials are no longer tightly tied to the security policy for that user. The access control is simply tied to the end-point security assessment information.

This lack of symmetry between 802.1X versions of Cisco's Network Admission Control and UDP versions means that the attractive idea of a single enterprise policy server handling access control on the LAN, the WLAN, and over the IPsec and SSL VPNs is not part of Cisco's current architecture. A further symptom of this is the lack of wireless support in the free Cisco Trust Agent. If you want wireless 802.1X, you'll have to replace the freeware Cisco Trust Agent 802.1X with a different 802.1X supplicant. The real focus of the current version of Cisco's Network Admission Control is end-point security assessment--the authentication that comes out of the an 802.1X dialog is really a side-effect and not a core aspect of the entire system.

Policy Enforcement Points in C-NAC

As a dominant manufacturer of switches, routers, and VPN devices, Cisco has an aggressive and difficult task in incorporating Network Admission Control into their devices. Policy Enforcement Points appear in Cisco's architecture as Network Access Devices, and Cisco has pages and pages of documentation explaining what devices will support which of the different client scenarios, EAP over UDP and EAP over 802.1X. Summarizing those charts is difficult and subject to some disagreement: Cisco's competitors cite the requirement to upgrade all switches as a major disadvantage of Cisco's approach, while Cisco believes that the majority of enterprise customers who will be interested in NAC already have the right equipment in place to start using it immediately. One very clear issue is that the policy enforcement capabilities vary widely between different devices. Sending full access control policies will only be possible in networks with very limited sets of devices. Instead, Cisco's support of more coarse-grained access control, such as VLAN-based or even simply "go/no-go," is really a focus of the products available today.

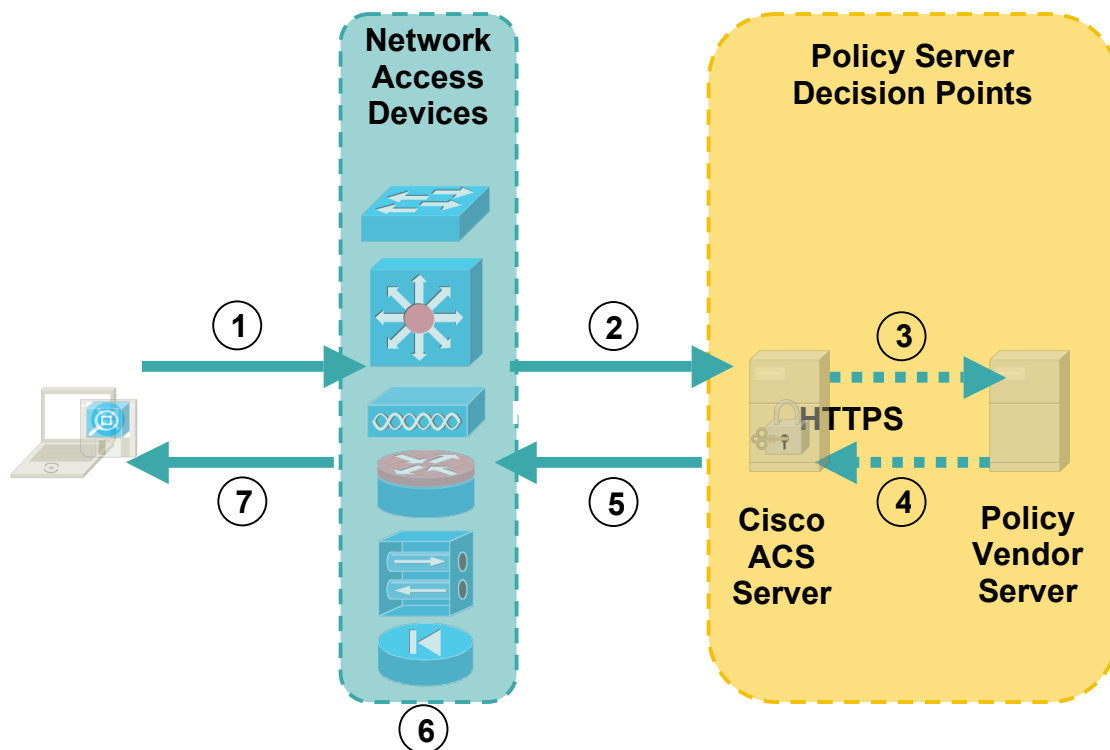
Cisco also offers a different approach to Network Admission Control with their Cisco Clean Access appliance (part of the Perfigo acquisition). Clean Access is also a part of their NAC strategy for people who want to have end-point security assessment, but who don't really want to change anything about their infrastructure. The long-term integration between the Clean Access server, the Clean Access agent, and NAC is uncertain.

Policy Decision Points in C-NAC

The back-end Policy Decision Point is composed of Cisco's own ACS (Access Control Server), along with interfaces to vendor-supplied policy servers, authentication servers, and audit servers. ACS, version 4.0 or higher, represents the Cisco version of a Network Access Authority combined with the Server Broker. Posture Verifiers, called Policy Server Decision Points in Cisco's architecture, connect to the ACS server using Cisco-defined protocols.

Cisco goes further than many open Network Admission Control architectures by including the concept of Audit Servers in its NAC architecture. The purpose of Audit Servers, in this context, is to audit the end-point security status of devices that do not have the Cisco Trust Agent installed on them. When an agent-less system tries to connect to a network protected by Network Admission Control, the Policy Enforcement Point can detect that there is no agent and then sic an Audit Server on the end system, either by trying to scan the system from the outside or by trying to download some agent software into the browser which will allow an audit to occur. Although the Audit Server aspect of Cisco's approach certainly fills an architectural hole, it's not very clear how much useful data the audit server will be able to collect and whether this will be sufficient to set network access policies.

Cisco's Network Admission Control is a serious one, backed up by products and support throughout Cisco's product line. From a purely architectural point of view, there are some ugly spots, such as the lack of policy integration when using non-802.1X methods. However, by responding to what must be an overwhelming set of conflicting customer demands, Cisco has made a good balance between what is architecturally elegant and what works in existing enterprise networks. If there is a weak spot in Cisco's architecture, it's the intense focus on end-point security and relative inattention paid to fine-grained access controls and authentication.



- 1) Host sends credentials to Access Device using EAP (UDP or 802.1X)
- 2) Access Device forwards credentials to Policy Server (ACS) using RADIUS
- 3) ACS Server authenticates and passes posture information to Policy Vendor Server
- 4) Vendor Servers respond with Compliant/ Non-Compliant Messages
- 5) Policy Server responds to Access Device with access rights and VLAN assignment
- 6) Access Device accepts rights, enforces policy, and (7) notifies client