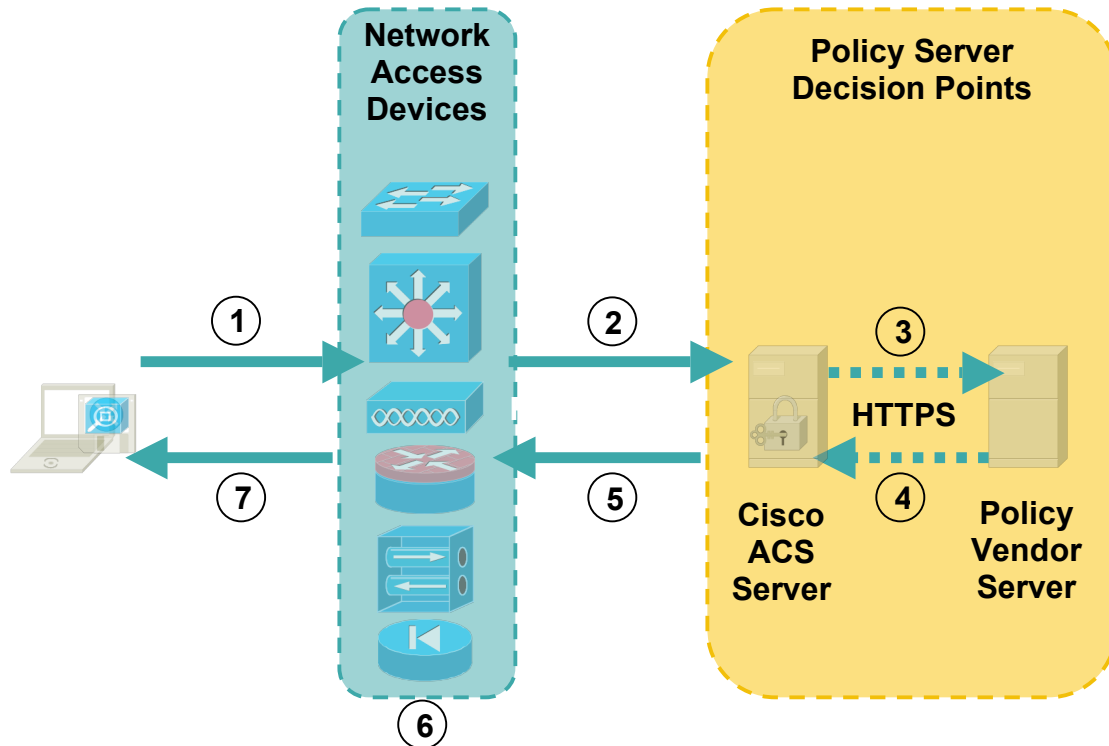


# What is Cisco NAC?

Cisco's Network Admission Control, which we'll call CNAC to avoid overloading the acronym NAC (for Network Access Control), maps directly to the IETF and TCG TNC architectures. Cisco has published a set of architectural overviews, supported product tables, and deployment guides at <http://cisco.com/go/nac/framework/>. This white paper is derived from some of those overviews as well as the results of our iLabs testing. You may find it helpful to have our companion white paper, "Network Access Control Architecture Alphabet Soup," in hand showing the diagram with different parts of a NAC architecture.



- 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

## Client Side (Access Requestor) CNAC

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 the Cisco Trust Agent (CTA), which is free software for wired 802.1X connections. For both wired and wireless connections, CTA works with Cisco Secure Services Client (CSSC) to provide posture credentials. The Posture Collectors are vendor-provided agents including support for the optional Cisco Security Agent (CSA), a Host Intrusion Prevention tool. The Interop Labs is demonstrating integration with CSA, Trend Micro, and LANDesk as 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 extended EAP functionality in EAP-FAST (Flexible Authentication via Secure Tunneling). With EAP-FAST in place, Cisco can include both IEEE 802.1X authentication as well as end-point posture compliance information in the EAP protocol. In order to do NAC at layer 2 (L2) or layer 3 (L3), the CTA has support for both EAP-over-802.1X and the proprietary EAP-over-UDP (EoU). This allows the same EAP-based identity and posture credentials used within 802.1X challenges to work over layer 3 (L3) connections for VPN, remote office, or any L3 connections.

There is a critical difference between the 802.1X and UDP versions of Cisco's EAP, however. In the 802.1X case, EAP includes both identity and security assessment information while EoU does not carry identity information. Instead, the user identity and security assessments are done in separate authentication transactions. 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 currently part of Cisco's current architecture.

### **Policy Enforcement Points in CNAC**

As a dominant manufacturer of switches, routers, and VPN devices, Cisco has a large number of devices to incorporate Network Admission Control into. Policy Enforcement Points appear in Cisco's architecture as Network Access Devices (NADs) at both L2 and L3 for coverage across all network edges as well as deployment flexibility with security assessment enforcement. 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 of the major focuses of Cisco device functionality is to go beyond basic VLAN or ACL assignment for a given security assessment. This is because like many other things in life, you will spend 80% of your time worrying about the 20% of exceptions to these prescribed methods of authenticated network access. Whether dealing with agentless devices (IP phones, printers, photocopiers), multiple-hosts per port (hubs, IP phones and PCs, VMware), special timer settings (PXE boot, DHCP) there are feature options to handle these exceptional scenarios. Even the capability to handle a AAA outage with an administrator-configured VLAN is available for maintaining security with a minimum level of access.

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 CNAC**

The back-end Policy Decision Point is composed of Cisco's own Access Control Server (ACS), 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 the Cisco-defined Host Credential Authorization Protocol (HCAP) is for delegating credentials to posture verifiers.

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 agentless system tries to connect to a network protected by Network Admission Control, the Policy Enforcement Point can detect that there is no agent and send a request to ACS for agentless handling. The ACS can either authorize the host via MAC authentication bypass or make a request using the Generic Authorization Message Exchange (GAME) protocol to have the Audit Server dynamically assess the host for the appropriate level of authorization. An Audit Server will either scan the host or have the user download a browser object for assessment. 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 policies.