CHAPTER 1

Cisco Trust Agent Overview

Cisco Trust Agent (CTA) is a component of the Cisco Network Admission Control (NAC) program. NAC enables network access devices to permit or deny network clients access to the network based on the posture of the software on the host. This process is called posture validation.

This chapter contains the following sections:

Cisco NAC Overview

The four main components of the Cisco Trust Agent (CTA) posture validation process are as follows:

- **Network client running Cisco Trust Agent**—Cisco Trust Agent collects security posture information from the NAC-compliant applications running on the network client and reports them to the Cisco Secure Access Control Server (ACS). These are some NAC-compliant applications:
  - Antivirus applications
  - Personal firewalls

  - Host-based intrusion protection applications, such as Cisco Security Agent (CSA)

- **Network Access Device (NAD)**—The NAD permits or denies network access. Typically, the NAD is a Cisco router or switch.
- **Authentication Server (Cisco Secure Access Control Server (ACS))**—The authentication server is responsible for obtaining and evaluating the security posture credentials from a network client, determining the overall client posture, and providing the appropriate posture token and network access policy to the NAD based on the client's posture.
- **Posture Validation Servers (optional)**—Posture validation servers support Cisco Secure ACS in determining the overall system posture. They are typically third-party applications that support the validation of the security posture credentials for a specific NAC-compliant application. For example, an antivirus software company may prefer to maintain its own posture validation server rather than store and update posture validation information on Cisco's ACS server.

Posture Validation Process Overview

Initial Posture Validation Process

The following provides an overview of how the posture validation components work together during an initial posture validation process.

1. The computer sends a DHCP (Dynamic Host Configurative Protocol) request to obtain an IP address or an ARP (Address Resolution Protocol) request to convert an IP address into a physical address.
2. The Network Access Device (NAD), a Cisco network router or switch, requests a network access policy from the Cisco Secure Access Control Server (ACS).
3. ACS requests the computer's posture credentials from Cisco Trust Agent (CTA) which was previously installed.
4. CTA receives the security posture credential request and, in turn, prompts the posture plugins installed on the computer to gather the posture credentials from the NAC-compliant applications on the client.

5. CTA aggregates all of the posture credentials from the client and returns the information to the NAD.
   - If the posture credentials are sent using the EAP over UDP protocol, the posture information is sent directly from the CTA to ACS.
   - If the posture credentials are sent using the IEEE 802.1x protocol, CTA hands the posture credentials to the Cisco Trust Agent 802.1x Wired Client, also known as the "supplicant" and the CTA 802.1x Wired Client forwards the information to the ACS. (See Chapter 9, "Cisco Trust Agent 802.1x Wired Client" for more information on the supplicant.)
6. ACS evaluates the security posture credentials for each application that resides on the computer. ACS can perform the credential evaluation using rules in the local database or can relay application credentials to an application-specific posture validation server for evaluation. The result of the evaluation is an application posture token for each evaluated application and an optional user notification.
7. ACS aggregates the application posture credentials and defines an overall system posture token for the client. The system posture token equals the least trusted posture of all the application posture credentials collected from the client.

   These are the default system posture tokens; they are ranked from the most trusted posture to the least trusted posture:
   - Healthy
   - Checkup
   - Quarantine
   - Transition
   - Infected
   - Unknown
8. ACS maps the system posture token to a network access policy an, optionally, a user notification.
9. ACS sends the result of the security posture validation back to the NAD, along with the appropriate network access policy for that client, and any user notification, back to the NAD.

10. The NAD implements the security policy for the client and forwards the posture information back to CTA on the computer. Depending upon how you have configured CTA, the results of the posture validation are logged and any user notifications are displayed on-screen in a dialog box.

    Based on the access policy, the network client is permitted on the network, denied access to the network, or quarantined to a remediation network until the NAC-compliant applications have been updated to the required levels.

Posture Revalidation Process

Posture revalidation is caused by one of three events and once it occurs posture is validated following the same workflow as described in Posture Validation Process Overview, starting with step 2.

Network Access Device Requests New Posture. In the case of NAC L2 IP or NAC L3 IP network admission methods, switches and routers maintain the posture for a configured amount of time and then that posture expires. When the posture expires, the NAD requests posture again.

An Internal Timer in CTA Expires. The SQTimer parameter defines the interval at which CTA requests the posture plugins for their status. If a posture plugin reports a change in posture status to CTA, CTA alerts the network access device, which triggers a re-posturing of the host. This is one implementation of the asynchronous posture status query feature.This feature is only available if CTA 802.1x Wired Client is installed on the host machine.

See "Configuring Asynchronous Posture Status Query" section on page 5-19 for more information on how to configure the SQTimer.

Posture Plugins Detect a Change in Status. Some posture plugins monitor the status of their applications and report status changes to CTA upon detection. Such plugins are considered "asynchronous" plugins. When CTA receives the status change from an asynchronous plugin, CTA alerts the network access device, which triggers a re-posturing of the host. For example, the posture plugin for Cisco Security Agent (CSA) detects when the CSA security has been turned off. This is one implementation of the asynchronous posture status query feature. This feature is only available if CTA 802.1x Wired Client is installed on the host machine.

Cisco Trust Agent Deployment Considerations

Network clients are the hosts on your network. This includes PCs, laptops, workstations, and servers. You may have hundreds or thousands of network clients on which you are going to install CTA. Installing and configuring CTA on that many network clients can be a time-consuming process.

To decrease the time spent installing and configuring CTA throughout your network, you can create a custom installation package. The custom installation package lets you provision the CTA settings at installation time. These settings include:

- Communication settings
- Posture notification settings
- Logging and notification setting
- Authentication policies for the CTA 802.1x Wired Client