CHAPTER 2

Cisco NAC Profiler Architecture Overview

Topics in this chapter include:

Overview

Cisco NAC Profiler is a modular, network appliance-based system that provides two top-level functions critical to the effective and efficient deployment and management of Network Admission Control (NAC) solutions. Those two functionalities are Endpoint Profiling and Behavior Monitoring. NAC Profiler performs these functions utilizing a unique approach and technologies that are both highly reliable and result in negligible impact to the endpoints and network. NAC Profiler performs the Endpoint Profiling and Behavior Monitoring functions by passively analyzing network traffic and several other methods described in the previous chapter to classify endpoints into an appropriate Profile according to pre-determined criteria or rules that guide the classification of all endpoints into the appropriate Profile. In addition, the system reports changes in endpoint connection status and stores the data for future retrieval. It also allows the user to take action with respect to changing selected port parameters of edge network infrastructure devices, parameters pertinent to the implementation and ongoing management of authentication and NAC solutions. All of these functions are controlled by the administrator using the web-based graphical user interface (GUI) accessible through a standard browser.

The Endpoint Profiling software that powers Cisco NAC Profiler is provided as two functional systems that reside on different appliances; the NAC Profiler Server and the NAC Profiler Collector. The NAC Profiler Server houses the database that contains all of the endpoint information, gathered from the associated Collectors, including device type, location, and behavioral attributes. In addition the Server presents the web-based GUI and liaises with the Clean Access Manager to keep the CAM's filters list current and relevant. There are also Forwarder modules that serve as middleware and facilitate secure communications between the Server and the Collectors. Finally, the Server also provides a module that can receive and analyze data from other sources such as Netflow records exported from Netflow-enabled infrastructure devices (e.g., routers) or other Netflow collectors. This information is combined with the information gathered from the Collectors and is used to further profile the network attached endpoints.

The NAC Profiler Collector resides on the same appliance with the Cisco's NAC Appliance Server and consists of a number of software modules that discover information about the network attached endpoints including a network mapping module (NetMap), an SNMP trap receiver/analyzer (NetTrap), a passive network analysis module (NetWatch), and an active inquiry module (NetInquiry). The major functions of the Profiler Collector are to gather all of the salient data about the endpoints communicating

to/through that Clean Access Server (CAS), and to minimize and aggregate the information that is sent over the network to the Profiler Server. Table 2-1 and Table 2-2 summarize the functions of the Profiler Server and the Collector.

Table 2-1 NAC Profiler Server Modules

NAC Profiler Server Module	Purpose
NetRelay	Receives endpoint profiling and behavior monitoring data from other systems, such as Netflow
Forwarder	Facilitates communication between all NAC Profiler modules, acts as middleware between Collector modules and the Server module in a NAC Profiler system
Server	Controller, modeling engine, GUI and database. Collects, classifies and logs incoming data. Serves web-based User Interface, and manages the Device Filters list in the Clean Access Manager for Cisco NAC Profiler systems.

Table 2-2 NAC Profiler Collector Modules

NAC Profiler Collector Module	Purpose
NetMap	Collector Module that queries network devices via SNMP for: • System information • Interface information • Bridge information • 802.1x information • Routing/IP information Builds and maintains a model of the network topology
NetTrap	Receives selected traps from network devices to assist NetMap in maintaining the model of the network topology
NetWatch	Passive network analyzer collector modules. Collects information about endpoints using network traffic
NetInquiry	Active profiling Collector module
Forwarder	Facilitates communication between all NAC Profiler modules, acts as middleware between Collector modules and the Server module in a NAC Profiler system

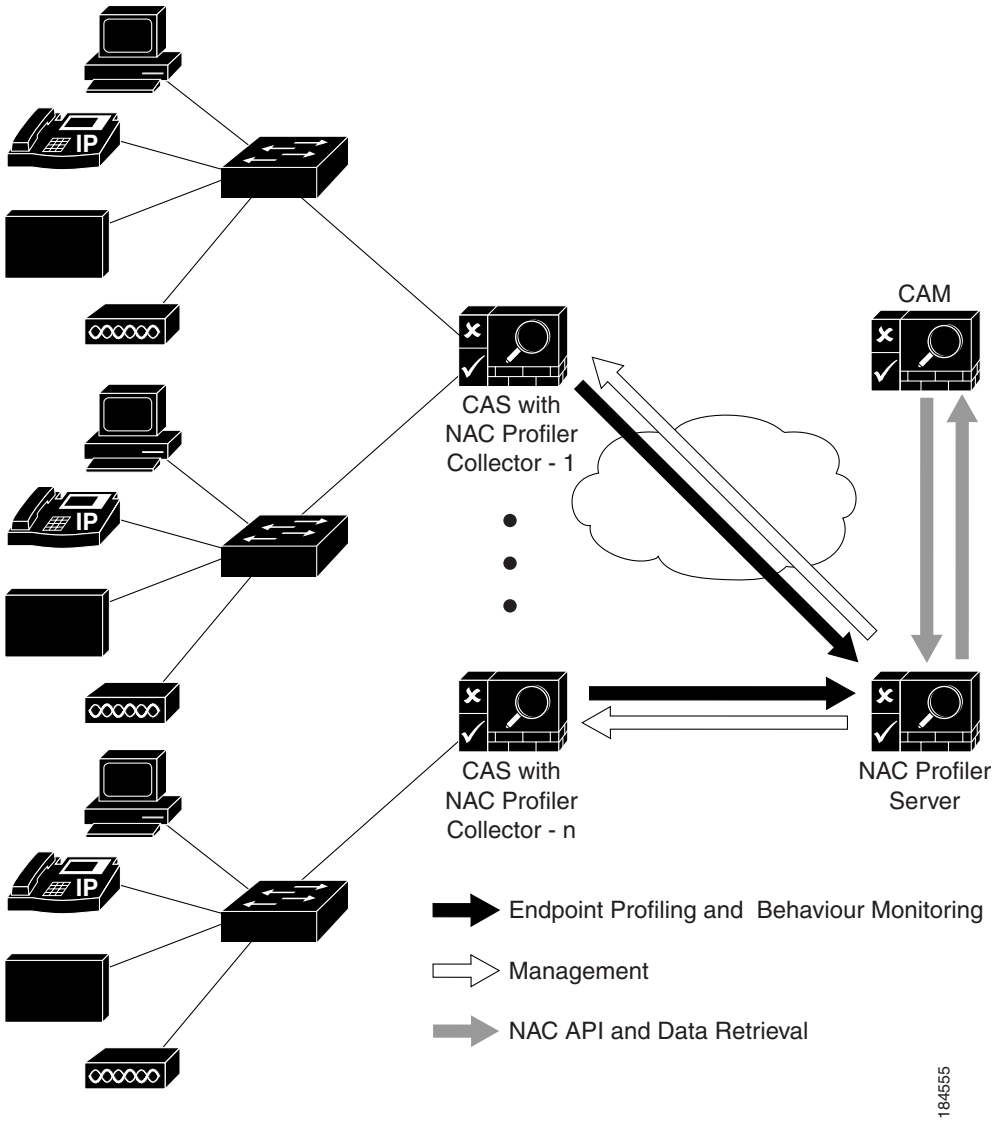
NAC Profiler System Deployment Model

Cisco NAC Profiler is designed and implemented as a modular system that employs one or more remote Collectors that distribute the data gathering to each CAS in the network, and provide distributed points of visibility while centralizing the Endpoint Profiling and Behavior Monitoring functions onto a centralized NAC Profiler Server. The remote Collectors run one or more instances of the desired collector module or modules plus the Forwarder system module. The Forwarder module on a Collector appliance forwards data collected by the remote appliance to the designated NAC Profiler Server. The Profiler Server aggregates the data received from all the collectors in the system and provides centralized management of the distributed NAC Profiler system.

Note Cisco NAC Profiler Collectors must be combined with a Cisco NAC Profiler Server in order to be managed, so that Endpoint Profiling and Behavior Monitoring data is aggregated analyzed, presented, and the appropriate endpoints sent to the Clean Access Manager's Device Filters list.

Figure 2-1 shows the NAC Profiler system, where one or more Collectors are deployed in conjunction with a central NAC Profiler Server. The Collectors send their Endpoint Profiling and Behavior Monitoring data to the central appliance via the onboard Forwarder module (blue lines), and are managed by the central appliance (yellow lines). Communications between the appliances is accomplished over the local or wide area network via an encrypted TCP session using the Management interfaces on the NAC Profiler appliances. The central appliance maintains the endpoint database and provides centralized management for the entire NAC Profiler system via the web based UI served by that appliance. The endpoint data that is denoted as needing to be provisioned to the Clean Access Manager is sent using the NAC API and data mining of the NAC Profiler database is performed via a web-based session with the Profiler Server.

Figure 2-1 Distributed NAC Profiler System



NAC Profiler Usage: Port Provisioning and Endpoint Directory

The Endpoint Profiling and Behavior Monitoring functions provided by the NAC Profiler are essential to the efficient and effective deployment and ongoing management of NAC in enterprise networks. The modes of operation for NAC Profiler can be categorized at the top level as Port Provisioning and Endpoint Directory.

The Port Provisioning functions of the NAC Profiler are used as an augmentation to the network management platform, providing purpose-built configuration management tools designed to assist with deployment and ongoing management of NAC in enterprise networks. Port Provisioning provides the network administrator with a UI for interacting with the edge network infrastructure devices (e.g., switches), and allows the manipulation of port parameters on those network edge devices providing access to a selected endpoint or group of endpoints for the purpose of provisioning authentication and or NAC-specific parameters. NAC Profiler utilizes SNMP communications or the CLI to make persistent configuration changes on selected ports of selected edge devices enabling network managers to have fine-grained control of the infrastructure providing endpoint connectivity. If port provisioning is not intended to be used, but SNMP is intended to provide discovery functionality on the Collectors, then read-only access is required. Read-write credentials are only required if port provisioning is to be used.

In the Endpoint Directory, Cisco NAC Profiler provides endpoint information to the CAM, most frequently managing the list of those endpoints that are unable to interact with the NAC system directly. In this usage mode, the NAC Profiler is integrated with the CAM using the methods described in Chapter 11, “Integration with Cisco NAC Appliance”, providing valuable and up-to-date information about non-user devices so that they can be provided reliable and secure access in an automated and dynamic fashion, regardless of their physical location.

In most NAC Appliance environments, the port provisioning function is only used at deployment time and when something acute needs immediate attention. The uses of this function at deployment time are to rapidly deploy VLAN port configuration settings to the network access devices so that they may communicate with NAC Appliance. These settings can be deployed by network switch by providing a list of ports on a device or by endpoint type whereby the GUI presents all of the endpoints of a give type in one table for configuration. This can be especially helpful when deploying NAC incrementally where it may be desirable to deploy certain device type (all windows users, all Apple users, etc) or certain groups of ports (all conference rooms or café ports).

The usage of the Endpoint Directory, meanwhile, is at the heart of the NAC Profiler/Clean Access interaction. The Endpoint Directory is a list of all profiled and un-profiled endpoints that are known to the NAC Profiler. From this list, the selected endpoint types (profiles) can be provisioned to the CAM. As new devices are discovered they can be added to the list. Endpoints that have been retired, or are found to be behaving in ways not appropriate for their known device type can be removed from the filters list.