CHAPTER 1

# Introduction to Cisco NAC Profiler

Topics in this chapter include:



## Overview

Cisco NAC Profiler enables network administrators to efficiently deploy and manage Network Admission Control (NAC) in enterprise networks of varying scale and complexity by identifying, locating and determining the capabilities of all attached network endpoints, regardless of device type, in order to ensure and maintain appropriate network access. Cisco NAC Profiler is an agentless system that discovers, catalogs, and profiles all endpoints connected to a network.

As networks grow larger, it becomes increasingly difficult to know with certainty which devices and device types are connected to each edge port. This can impede the deployment and ongoing management of the enterprise network after implementation of a NAC edge security solution. In order to provide constant, reliable and secure access to all authorized endpoints regardless of their respective capabilities, it is essential to know whether or not each endpoint at the edge of the network can interact with the authentication or NAC solution deployed. Providing the capability in a way that minimizes administrative burden and is inherently dynamic are prerequisites to successful deployment and operation of edge security solutions, particularly in large-scale enterprise networks.

Typically, devices such as printers, FAX machines, IP telephones and Uninterruptible Power Supplies, typically are not capable of running a NAC client. This means that in the deployment of NAC solutions, special purpose devices such as these do not have an agent available, nor do they provide a means by which a user can manually intervene through a browser. In this case, the ports connecting these endpoints must either be provisioned to circumvent the NAC system (e.g., placed on a special VLAN) or alternatively, the NAC system configured to recognize these devices via their unique hardware address in order to provide them access without direct participation in the admission control protocol. This typically requires that the NAC system be made aware of these endpoints by MAC address so that they can be admitted based on that credential alone with no further interaction with the NAC system. In the case of Cisco NAC Appliance, non-NAC devices such as these are accommodated via the Device Filters list of the Clean Access Manager.

Cisco NAC Profiler provides Endpoint Profiling and Behavior Monitoring functions to allow administrators to thoroughly understand the types of devices connecting to the network, their location and their abilities relative to the state of the port on which they currently reside. Endpoint Profiling and Behavior Monitoring can be deployed in enterprise networks ranging from hundreds to tens of thousands of users. The following overviews provide background on these core functions of Cisco NAC Profiler.

# Endpoint Profiling Overview

Endpoint Profiling records a network endpoint's observable behaviors, analyzes its identifiable characteristics in order to classify it to a particular group (Profile), and assesses its ability to participate in a certain sphere, such as a given authentication or network admission control (NAC) solution. In essence, Endpoint Profiling ia behavior-based characterization of endpoints for the purpose of identifying and grouping together those that are similar in function, capability or other defining characteristics.

NAC Profiler classifies or profiles each endpoint it discovers and locates on the network into exactly one Profile according to the passive and active profiling mechanisms of the endpoint profiling engine. Each Profile is a logical container or grouping that contains one or more endpoints with similar behavioral-based characteristics (e.g., printers, IP Phones, game consoles, etc.) and similar ability to comply with the authentication, NAC or other requirements placed on the endpoints in a network.

Each endpoint connected to the enterprise network either can or cannot interact with the authentication or admission control system to gain access to the network. Endpoints such as Windows or Linux computers are generally able to meet all the requirements of authentication and NAC systems, while devices such as printers, security badge readers, manageable Uninterruptible Power Supplies (UPS) cannot.

Endpoint participation in authentication or admission control generally requires that the endpoint either submit credentials automatically (e.g., via a supplicant or agent running on the endpoint and properly configured with the correct credentials) or through manual user intervention (e.g., via entering user credentials manually via a web browser) in order to be authenticated successfully or admitted onto the network. Endpoints without this capability must be identified so that they are not subjected to authentication or admission control direct challenges.

In addition, enterprise networks can include systems that run Windows but do not participate in Authentication or NAC processes, because either they are federally regulated and their software images cannot be changed (biomedical devices for example) or because they are not user-centric devices (robotics, research, etc). Because these endpoints cannot respond to the challenge either automatically or through user intervention, alternate network provisioning must be performed to ensure these endpoints are provided with secure and reliable access to the network post-implementation of port based authentication or NAC. They are in fact authorized endpoints; however, their inherent limitations prevent them from being authenticated or admitted through interaction with the authentication or NAC system. In these kinds of enterprise environments, there can be an equal number of NAC-capable and non-NAC capable devices. Cisco NAC Profiler is designed to address such networks.

Cisco NAC Profiler performs dynamic Endpoint Profiling. Endpoint Profiling identifies and locates each endpoint on the network, groups those endpoints according to their capabilities or limitations, then allows accommodation of non-authenticating or non-NAC endpoints through a choice of mechanisms: interacting with the network infrastructure directly to allow manual re-provisioning, or acting as a directory of non-authenticating or non-NAC capable endpoints.

The NAC Profiler directory allows an authenticator or NAC system to make a qualified decision about a particular endpoint. The authentication server or NAC system accesses the NAC Profiler directory via APIs or protocols such as LDAP to get real-time profiling intelligence about endpoints as they try to access the network.

Cisco NAC Profiler's Endpoint Profiling is inherently dynamic and can detect changes at the network edge resulting from network adds, moves and changes. New MAC or Profile Change events (see Chapter 10, "Configuring NAC Profiler Events") can be used to alert network or security operations and to enable re-provisioning required to effectively support moves, adds and changes in the authenticated or admission controlled network.

Cisco NAC Profiler's Endpoint Profiling provides the network administrator visibility into the state of the network down to the endpoint and network port level. Cisco NAC Profiler's reporting features provide real-time operation status for each switch port in the network, the endpoints connected to them, and the current Profile assigned. Cisco NAC Profiler maintains a historical record on each endpoint so that location, logical addressing and Profile information can be easily recalled for purposes such as security event management forensics.

# Endpoint Behavior Monitoring

Non-authenticating or non-NAC endpoints need to be monitored over time to ensure that their behavior is consistent with their known device type. Profiles are a device type classification that enable the appropriate level of network access without requiring authentication credentials. Typically, endpoints that cannot authenticate or participate in network admission control are special purpose devices (such as printers, IP phones, wireless access points, UPS or HVAC devices) that provide a dedicated service on the network. When special-purpose endpoints begin to exhibit behaviors of general purpose computing devices (such as desktop and laptop computers), behavior monitoring detects this. For example, behavior monitoring can detect MAC spoofing, one of the more rudimentary methods used to gain unauthorized network access.

Cisco NAC Profiler's Behavior Monitoring continuously collects and analyzes behavior information for all endpoints utilizing the network. When the behavioral attributes of an endpoint change, the NAC Profiler engine evaluates whether or not the behavioral changes warrant a change in the Profile of the endpoint. If a change in Profile is warranted, NAC Profiler transitions the endpoint Profile and provides alerts to network and security management. In addition, NAC Profiler can automatically change the network access provided by the authentication or NAC system to deny access to the suspect device. In this way, Cisco NAC Profiler can automatically counter attempts to thwart the edge security system.

Whereas Endpoint profiling provides automated population of exception lists or white lists to accommodate non-authenticating and non-NAC nodes, Behavioral Monitoring provides an additional security mechanism as well as automated ongoing management of these critical elements of network authentication and admission control systems. The Behavior Monitoring functionality of NAC Profiler Adds a second credential to the known and authorized non-authenticating or non-NAC endpoints, that of a behavioral signature to ensure that the MAC address of these devices cannot be exploited as a means to bypass network authentication or admission control.

# Endpoint Profiling and Behavior Monitoring Strategies

Cisco NAC Profiler uses a number of mechanisms to establish and maintain a complete contextual inventory of all devices connected to the network, including their type and location (switch and port).

Cisco NAC Profiler does not operate in an "inline" mode, and does not require visibility of network traffic at every broadcast/Layer 2 domain on the network. Cisco NAC Profiler can operate effectively in a network segmented both at layer 2 via VLANs and at layer 3.

Cisco NAC Profiler Collector modules are deployed at aggregation points in the network where traffic between the endpoints and centralized services (e.g., application and print servers, Internet links, etc.) is accessible and can be redirected to a monitoring interface on the Cisco NAC Appliance Clean Access Server (CAS). For this reason, Collector modules are collocated on the CAS. The distributed Collectors aggregate endpoint information into the centralized Cisco NAC Profiler Server as described in Chapter 2, "Cisco NAC Profiler Architecture Overview".

Cisco NAC Profiler does not rely on any software agents loaded on the endpoints, nor does it require administrator-level access to endpoints in order to perform Endpoint Profiling or Behavior Monitoring. Cisco NAC Profiler instead relies on directly observable attributes of endpoint behavior on the network combined in some cases with information gathered from the network infrastructure devices (e.g. edge switches, routers, Netflow collectors, etc.) to perform its functions. In many environments, Cisco NAC Profiler can primarily operate in passive mode, but it also includes active components that can leverage standard information from network services (e.g., DNS) in a non-invasive fashion to Profile certain endpoints that are difficult to Profile passively.

Unlike other IT asset inventory discovery systems, Cisco NAC Profiler continually performs its functions and maintains real time and historical databases of information about endpoints in the environment. It does not operate on a "snapshot" basis that periodically scans the network to determine what is connected and characterizes endpoint types based on techniques such as port scanning. Cisco NAC Profiler continually monitors the behavior of each endpoint and updates its database based on data supplied by the Collector modules to evaluate which Profile the endpoint best matches. History is maintained on each endpoint to provide a summary view into the Profile(s) an endpoint has been in, the addresses it has used, and where it has been connected to the network.

It is often assumed that a NAC Profiler system, specifically the passive traffic analysis component, must be capable of high sustained throughput to process feeds of aggregated network traffic. Cisco NAC Profiler is never deployed in an inline mode and cannot become a bottleneck. Unlike an IDS or IPS that must examine essentially every packet that is presented to it in order to detect a potential attack on the network, Cisco NAC Profiler needs to examine only the packets that are useful for Endpoint Profiling and Behavior Monitoring. Cisco NAC Profiler therefore does not require massive throughput capabilities, and because it does not need to store all packet information to support forensic activities, its data storage requirements are relatively small.

Cisco NAC Profiler is flexible enough to provide Endpoint Profiling and Behavior Monitoring in just about any environment, even those where some of these capabilities are not practical. There are considerations and trade-offs when utilizing different sources of endpoint data. Depending on the networking environment, the level of granularity of Endpoint Profiling and the ability to provide Behavior Monitoring is proportional to the visibility and access granted to the system.

The NAC Profiler Collector operates at various levels of the OSI stack, beginning at layer 2. Cisco NAC Profiler tracks the individual endpoints discovered on the network by their physical network interface address (e.g., MAC address), and the registered manufacturer of that interface.

Cisco NAC Profiler primarily uses SNMP communication with the network infrastructure devices to discover all endpoints on the network. NAC Profiler regularly polls the switches and routers in the network via SNMP to determine what endpoints are connected to what ports, and what logical (IP) address each device is currently using. The NAC Profiler engine resolves the network topology down to the end nodes to develop a model or map of the network.

Cisco NAC Profiler communicates using the same protocol employed for enterprise network management, using Read Only mode to gather topological information from network devices at a configurable interval. Because NAC Profiler is interested in only a small subset of the Management Information Base maintained on these devices, the regular polling by NAC Profiler is not bandwidth intensive and does not impact the devices adversely. When SNMP polling is available, NAC Profiler can rapidly and accurately ascertain all endpoints present in the environment. In the absence of SNMP, NAC Profiler relies on other means to build out the list of devices in the environment.

Cisco NAC Profiler leverages SNMP traps from the edge infrastructure when available to detect changes in the endpoint topology in near real-time. NAC Profiler uses Link State traps to determine when endpoints join or leave the network in order to immediately poll affected devices to re-map the network topology. When SNMP traps are not available, NAC Profiler uses a series of timers to obtain network change information. This can result in potential delays in the system's ability to respond to network changes in real time, but in practice the timers provide the necessary functionality to track the movement of endpoints.

Cisco NAC Profiler is also able to track and utilize the logical (IP) addressing of endpoints as a criterion for Profiling. NAC Profiler continually tracks the physical-to-logical address bindings of each endpoint, and rules can be created that associate endpoints using specific addresses with a device type. This enables a straightforward approach to Profiling statically-addressed devices such as network infrastructure or other devices that are known to be addressed from a reserved pool of host addresses.

When NAC Profiler Collector modules are provided with redirected network traffic, typically aggregated traffic between the endpoints and the segments serving the shared services (e.g., data and application servers, Internet link, etc.), NAC Profiler can perform profiling based on observable attributes of endpoint behavior at the network layer and above. Cisco NAC Profiler is provided access to network traffic from these segments via traffic redirection (for example, mirror ports, SPAN, RSPAN, and so on) to deliver network traffic to a monitoring interface on a NAC Profiler appliance running the NetWatch module.

In addition to these discovery mechanisms that reside on the Collector, the NAC Profiler Server can process Netflow export data records from Netflow collectors already deployed in the network. By examining network traffic directly, or traffic flow data, Cisco NAC Profiler can determine endpoint traffic patterns and other characteristics that can be employed to make Profiling decisions, such as the IP address rules discussed in the above paragraph and other rule types that operate at Layer 4 and above. Some examples of using endpoint traffic or flow data for Endpoint Profiling are provided below:

- NAC Profiler can identify endpoints that communicate with a service (e.g., TCP or UDP port) with certain resources. For example, network printers can be observed communicating with a print server on TCP port 9100.
- NAC Profiler can positively identify certain devices based on the observation of the endpoints running identifiable software agents. For example, Windows devices can be identified by the presence of web browser agents when the station opens a web browser when going to a website.
- NAC Profiler can identify different server types by observing server banners.

NAC Profiler is also able to glean information from network services such as DNS and DHCP. In the case of DHCP, NAC Profiler can process DHCP requests from endpoints utilizing the protocol. DHCP requests can be examined for client name and or client vendor information to be used in Profiling. DHCP requests from the segments providing endpoint connectivity can be delivered to the NAC Profiler collector in one of two ways:

- A monitoring interface on a NAC Profiler appliance can have the traffic from the LAN segment supporting the DHCP server(s) redirected to it. In this mode, all DHCP requests from endpoints are received by the monitor interface and examined for the client name or client vendor information.
- Alternatively, DHCP redirection (sometimes referred to as IP Helper addressing) on the LAN-facing router interface can be utilized to forward a carbon copy of all DHCP requests from the LAN(s) served by that router interface directly to the management interface on a NAC Profiler interface. NAC Profiler does not get involved in the DHCP protocol directly, it simply utilizes these redirected unicast copy of the DHCP requests to gather Profiling data.

In environments where the passive techniques are not sufficient to Profile 100% of the endpoints, Cisco NAC Profiler can utilize a variety of active Profiling techniques. Active profiling capability is an option that can be used in certain environments, particularly in cases where there are statically addressed endpoints that do not regularly communicate with centralized services. Cisco NAC Profiler active profiling capabilities are significantly different from other tools repurposed for endpoint discovery. For example, Cisco NAC Profiler does not utilize an active scanner that subjects endpoints to a barrage of traffic to determine what ports a given endpoint will open. Rather Cisco NAC Profiler allows the administrator to configure several selective probes of selected endpoints themselves or network services such as DNS in order to gather Profiling data actively. The active Profiling capability for example can be used to have the NAC Profiler appliance itself initiate a connection on a TCP port with endpoints on a target segment. NAC Profiler can attempt to establish a session on a given TCP port with a specified set of stations, and the success or failure of that attempt is captured on the NAC Profiler appliance interface in order to induce traffic which can be in turn utilized as described earlier in the document. In addition to attempting to actively create TCP sessions with designated endpoints, active Profiling can be used to query DNS to get the hostnames of selected endpoints as well as request web and SMTP server banners. Rules using these parameters can then be utilized with the actively generated traffic as well as that being collected passively utilized by the NAC Profiler engine to find matches and assign endpoints to the correct Profiles.