CHAPTER 3

Preparing for Deployment

Topics in this chapter include:

- Overview, page 3-1
- Preparation Steps, page 3-1
- NAC Profiler System Configuration Workflow, page 3-6

Overview

Before deploying and configuring Cisco NAC Profiler, there are a number of planning tasks to complete, based on how Cisco NAC Profiler will interact with the existing infrastructure.

As outlined in Chapter 2, "Cisco NAC Profiler Architecture Overview", the Cisco NAC Profiler system consists of a Cisco NAC Profiler Server which is a standalone appliance, and one or more NAC Profiler Collectors that run on the Clean Access Server appliances (NAC-3310 or NAC-3350) deployed as part of the Cisco NAC Appliance system.

Chapter 2, "Cisco NAC Profiler Architecture Overview" provided an overview of Endpoint Profiling and Behavior monitoring emphasizing the flexible nature of Cisco NAC Profiler and the strategies that may be employed in engineering an Endpoint Profiling and Behavior Monitoring system that meets the needs of the overall Cisco NAC Appliance deployment. The various data collection techniques outlined can be selected and combined to create a system that utilizes the sources of endpoint data that can be provided to it in each environment.

Preparation Steps

The following steps guide the collection of data and considerations to be taken into account prior to implementing Cisco NAC Profiler in a given enterprise network. Note that this list is not exhaustive. There are other options such as the use of external data sources such as Netflow, and the options to use the NetInquiry module for Active Profiling of endpoints. These topics are covered in later chapters of this guide. The following steps are designed to assist with the initial configuration of Cisco NAC Profiler systems that can be built upon via tuning of the system and employment of optional capabilities.

Step 1 Determine NAC Profiler Server IP Configuration, page 3-2

Step 2 Internal Network Address Blocks, page 3-2

Step 3 Network Device List, page 3-3

Step 4 DHCP Traffic Analysis, page 3-3

Step 5 Monitoring Interface Requirements, page 3-4

Step 6 SNMP Trap Configuration, page 3-4

Step 7 Determination of Required Profiles, page 3-5

s

Determine NAC Profiler Server IP Configuration

Cisco NAC Profiler is managed via secure HTTP. The Cisco NAC Profiler Server manages the Profiler system management, and the system components (e.g., Server and Collector(s) communicate with one another and with network devices and other components via TCP/IP.

The Cisco NAC Profiler Collectors use the same network interface on the appliance used by the Clean Access Server. The NAC Profiler Server must have the management interface on the appliance (eth0) configured with the necessary TCP/IP addressing and other parameters to enable IP connectivity in the environment.

Determine the following operating environment-specific parameters for the Management Interface of NAC Profiler Server appliance:

- IP host address and netmask
- IP address for the default gateway to be used by the system
- IP address of the Name Server

The IP address of the NAC Profiler Server is required when performing the initial configuration of the NAC Profiler Collectors. It needs to be determined prior to initial NAC Profiler Collector startup as described in Chapter 4, "Installation and Initial Configuration".

In addition, the IP addresses of each of the CAS appliances running the NAC Profiler Collectors should be determined and noted. This will facilitate the configuration of the NAC Profiler Server as described in Chapter 6, "NAC Profiler Server Configuration".

Consider any ACLs or other potential issues with network communication between the NAC Profiler Collectors and the network devices (e.g., switches and routers), and the computer that will be used to manage Cisco NAC Profiler via HTTPS. SSH is utilized for command line access to Cisco NAC Profiler over the network so enabling SSH access from the management computer to the NAC Profiler Server and Collectors should also be considered.

Internal Network Address Blocks

The NAC Profiler configuration specifies the range of host addresses of the devices that should be Profiled by the system. These address blocks consist of typically one or more IP subnets or networks that are used for assigning host IP addresses to the endpoints on the physical network for which NAC Profiler will provide Endpoint Profiling and Behavior Monitoring. This prevents the system from maintaining profile information on endpoints with source addresses outside the address space controlled by the organization.

Collect the address block(s) (CIDR format: x.x.x.x/mask bits) that specify the host addresses of all the endpoints to be profiled in the network(s) targeted for the NAC Profiler deployment.

Network Device List

NAC Profiler models the network infrastructure and communicates with the network infrastructure devices (switches and routers) via SNMP to gather information about the network topology when available. In order to utilize this functionality, Cisco NAC Profiler must be provided a list of the IP addresses of the network devices, and SNMP Read Only community strings in order to enable this communication. If SNMP is not enabled on the edge devices, it is recommended that SNMP be enabled in order to allow polling by Cisco NAC Profiler in order for the system to maintain a model of the network topology.

A list of network devices (switches and routers) that provide connectivity to the endpoints to be profiled should be compiled including IP address, device name, and read-only community string, preferably in a spreadsheet in CSV format to facilitate the data entry task.

Chapter 8, "Adding Network Devices to the NAC Profiler Configuration" describes the addition of network devices to Cisco NAC Profiler configuration in detail.

Many Network Management software solutions provide the capability to export device lists in CSV format with the information required by Cisco NAC Profiler. NAC Profiler provides the capability to import network device information provided in CSV format.

For basic, read-only connectivity with read-only devices compile a list of network devices in a CSV file formatted as follows:

```
 DeviceName1,IP1,ReadOnlyCommString
 DeviceName2,IP1,ReadOnlyCommString
...
```

If NAC Profiler will be used to provision infrastructure devices to facilitate network management tasks associated with the deployment and management of NAC as described in Chapter 2, "Cisco NAC Profiler Architecture Overview", the Read-write community string must also be provided so that NAC Profiler can perform SNMP sets to network devices.

In order to use NAC Profiler in the port provisioning mode, create a list of network devices in a CSV file formatted as follows:

```
 DeviceName1,IP1,ReadOnlyCommString,ReadWriteCommString
 DeviceName2,IP1,ReadOnlyCommString,ReadWriteCommString
...
```

DHCP Traffic Analysis

Cisco NAC Profiler can utilize DHCP requests from endpoints as sources of data for Endpoint Profiling. If some or all of the hosts to be Profiled are using DHCP for their addressing, consideration should be given to making DHCP requests from endpoints visible to Cisco NAC Profiler. If Cisco NAC Profiler is not able to collect the DHCP requests directly (e.g., not on the same LAN as the hosts using DHCP) a way to accomplish this is the use of the IP Helper Address used to redirect broadcast DHCP request packets from the router interfaces connecting the LANs to the rest of the network or by simply using SPAN or RSPAN to send the traffic from Ethernet ports to which the DHCP servers connect as described below in #5.

In the case of redirection, an IP-Helper address can be added to the configuration file of the router(s) specifying the appliance interface IP address of the desired NAC Profiler Collector that should process DHCP information (more specifically the NetWatch module on that NAC Profiler Collector). With this configuration, the router(s) forwards DHCP broadcasts not only to the DHCP server(s), but also to Cisco NAC Profiler for analysis for Endpoint Profiling and Behavior Monitoring purposes.

NAC Profiler does **not** get involved in the DHCP process regardless of how it receives DHCP requests. It simply passively collects the request packets and uses the data for the purposes of endpoint profiling and or behavior monitoring, and therefore has no effect on the DHCP service for the network.

Monitoring Interface Requirements

The NAC Profiler Collectors can utilize some of the triple-speed network interfaces on the NAC-3310 and NAC-3350 Clean Access Server (CAS) appliances to collect and analyze packets useful for Endpoint Profiling and Behavior Monitoring. These passive analyzer interfaces are used to gather network traffic for analysis by the NetWatch module running on the NAC Profiler collector. For both CAS models, the eth3 interface can be used to receive traffic of interest redirected via SPAN or RSPAN. In addition, the eth0 interface (management) of the appliance can also serve as a monitoring interface for the NAC Profiler Collector. Particularly in L2 deployments, this interface can yield useful data such as DHCP requests from the L2 boundary.

One of the most useful sources of endpoint profiling information for Cisco NAC Profiler is DHCP. If DHCP is in use in the environment, placing a monitoring interface on the link that services the DHCP server or servers can provide highly useful data to Cisco NAC Profiler. As an alternative, routers servicing the LAN segments can be configured with an IP helper-address as described inDHCP Traffic Analysis, page 3-3.

Consideration should be given to using the eth3 interface for receiving re-directed traffic (through the use of SPAN, RSPAN) of endpoint traffic traversing from the edge of the network to server farms and the Internet link which yield traffic useful for endpoint profiling and behavior monitoring.

Refer to Chapter 7, “Configuring Cisco NAC Collector Modules” for additional information.

SNMP Trap Configuration

Cisco NAC Profiler can utilize traps from edge devices in performing the Endpoint Profiling and Behavior Monitoring functions. It is recommended that network devices providing endpoint connectivity be configured to send SNMP Traps for Link State changes and MAC-address-change notification traps (the latter being available on only some vendor’s switches) to the NAC Profiler Collector. The NAC Profile Collector designated as trap receiver for a given device should be the same as that running the NetMap module responsible for regular polling of that device.

Ensure that infrastructure devices providing endpoint connectivity are configured to send Link State and New MAC traps to the IP address of the management interface of the NAC Profiler Collector running the NetMap module designated in the configuration for polling the device. Refer to the device manufacturer’s documentation for detailed instructions on the configuration of SNMP traps.

An illustrative SNMP trap configuration for Cisco IOS-based switches is provided below:

The following notes provide instruction for configuration access switches to send desired traps to Cisco NAC Profiler. The configuration commands shown are applicable to most Cisco IOS-based switches with the most recent releases of firmware. Some switches may not support all trap-types (notably, as of this writing, MAC-address-change notification traps are not supported by the Cisco Catalyst 6500-series of switches). For non-Cisco switches, consult the documentation for the device.

The following IOS commands will enable the sending of desired SNMP traps to Cisco NAC Profiler:

```
(config)# snmp-server enable traps mac-notification
(config)# snmp-server enable traps snmp linkup linkdown
(config)# snmp-server host <NAC Profiler-IP-address> traps version 1 <community-string>
mac-notification snmp
```

This will enable link-status traps for all interfaces and configure the switch to *potentially* send MAC-address-change notification traps. For MAC-address-change notifications to actually occur, the following command must be utilized for each interface of interest:

```
(config)# interface GigabitEthernet 2/29
(config-iface)#  snmp trap mac-notification change added
```

MAC-address-change notification should be enabled on access switch ports where endpoints connect. Of particular interest are ports connecting wireless controllers (such as the Cisco WLC). MAC-address-change notification should ***never*** be enabled on inter-switch links (e.g., trunk) ports.

The network devices should be configured such that Cisco NAC Profiler receives only Link State and MAC-address-change notification traps. Forwarding all network device traps to NAC Profiler is undesirable in that it provides no additional information to the system and can potentially negatively impact system performance.

Determination of Required Profiles

Profiles are logical containers used to discover, locate and classify devices into device-types or classes that have similar operating characteristics, capabilities, and limitations.

In networks where NAC will be deployed, the primary driver will be to discover, locate and classify all endpoints with particular attention paid to those endpoints unable to interact with NAC appliance. These are for the most part the non-Windows PCs and other devices for which there is neither a NAC agent available nor allow for user interaction with the NAC system via a web browser: devices such as printers, manageable Uninterruptible Power Supplies, game consoles and other special-purpose devices must be provided network access via alternative network provisioning. Identifying and locating these devices and enabling dynamic provisioning require the creation of Profiles for each of the device-types within the environment so they can be identified, located and tracked, and be provided network access in a manner which scales and preserves the integrity of the NAC implementation.

NAC Profiler ships with a number of Endpoint Profiles preconfigured based on deployment experience to date. Several of the existing profiles that ship preconfigured on the system may be applicable in the environment. The following are examples of preconfigured profiles:

- APC UPS
- Cisco WLAN Access Point
- HP Jet Direct Printer
- IP Phone
- Windows User
- Linux OS

As part of the preparation for the deployment of the product, the types of endpoint devices known to be connected to the network, the needs for a contextual inventory along with plans for authentication and or NAC deployment should be discussed and a preliminary list of the required profiles developed and discussed.

NAC Profiler System Configuration Workflow

System configuration of the NAC Profiler is a multi-step process. Prior to beginning implementation of the system, it is highly recommended that a system-level plan be developed. Of primary importance is understanding Cisco NAC Profiler components: how they will be addressed, where they will be placed in the network, and how polling of network devices will be distributed amongst the NetMap modules in the system running on the NAC Profiler Collector appliances (e.g., CASs).

This information should be well established prior to the startup of the NAC Profiler Server and the NAC Profiler Collectors that comprise the system. The startup procedure requires the input of these parameters as the system is setup and should be readily available by personnel performing the initialization as outlined in Chapter 4, "Installation and Initial Configuration".

Cisco NAC Profiler system management is provided through the NAC Profiler Server and accessed via standard web browser and HTTPS.

Table 3-1 represents the workflow for configuration of Cisco NAC Profiler. The remaining chapters in this guide provide instructions for completion of the configuration tasks described in Table 3-1. The workflow begins with completion of the appliance startup procedures for the NAC Profiler Server and the NAC Profiler Collectors running on the Clean Access Servers to be deployed in the system. Appliance start-up procedures are completed on each appliance using keyboard and monitor, or a terminal session. Detailed instructions for initial startup of NAC Profiler Server and Collector appliances are provided in Chapter 4, "Installation and Initial Configuration". Once the Server and Collector(s) have been initially configured, all further system configuration is completed via the web interface.

Table 3-1 Task Flowchart

Task	Description
1. Appliance Start-Up	Complete appliance start-up procedure for NAC Profiler Server and NAC Profiler Collector(s) by following procedures outlined in Chapter 4, "Installation and Initial Configuration". These steps initialize and address all components as well as enable network communications for all components. Establish web session with the NAC Profiler Server to complete system configuration.
2. My Networks Configuration	Chapter 5, "Configuring NAC Profiler for the Target Environment" outlines procedures for configuring Cisco NAC Profiler for the target environment and saving system configuration changes.
3. Configure NAC Profiler Server	Chapter 6, "NAC Profiler Server Configuration" outlines the configuration procedure for the NAC Profiler Server component. Complete the configuration of the NAC Profiler Server prior to adding the NAC Profiler Collector(s).
4. Add NAC Profiler Collectors	Chapter 7, "Configuring Cisco NAC Collector Modules" outlines the procedure for adding each of the NAC Profiler Collectors to the system, and the configuration of each of the software modules (such as the Forwarder, NetMap, NetWatch, NetInquiry, and NetTrap) that run on each Collector as required for the system.

Table 3-1 Task Flowchart

Task	Description
5. Configure Network Devices	Chapter 8, "Adding Network Devices to the NAC Profiler Configuration" outlines the procedures for adding the network devices to the system configuration. Polling of network devices is distributed amongst the NetMap modules running on the NAC Profiler Collectors in the system. Network devices and the necessary SNMP information are added or imported to the system configuration, and a NetMap module is designated to poll each device.
6. Configure Endpoint Profiles	Chapter 9, "Configuring Endpoint Profiles" outlines the procedures for enabling the endpoint Profiles included with the NAC Profiler, and for creating new Endpoint Profiles. The use of the rule types used in Profile creation for both passive and active endpoint profiling is outlined.
7. Configure NAC Appliance Integration	Chapter 10, "Configuring NAC Profiler Events" outlines instructions for enabling integration of the NAC Profiler Server and Cisco NAC Appliance CAM to enable automatic population and management of non-NAC endpoints.
8. Configure Endpoint Events	Chapter 11, "Integration with Cisco NAC Appliance" outlines instructions for enabling Endpoint Events and establishing communication between a NAC Profiler system and enterprise network and/or security management.
9. Configure User Accounts	Chapter 12, "Manage NAC Profiler User Accounts" outlines procedures for adding, editing, and deleting NAC Profile user accounts.

At this time, if the NAC Profiler Server and Collectors have yet to be initialized, collect the necessary information outlined in this chapter and proceed with initialization of the Server and each Collector as outlined in Chapter 4, "Installation and Initial Configuration".

At the completion of the initialization procedures, and the establishment of web management of the NAC Profiler Server, return to Chapter 5, "Configuring NAC Profiler for the Target Environment," to begin NAC Profiler system configuration.