Introduction

This chapter provides a high-level overview of the Cisco NAC Appliance solution. Topics include:

- What Is Cisco NAC Appliance?, page 1-1
- Cisco NAC Appliance Components, page 1-2
- Clean Access Server Features, page 1-6
- CAS Management Pages Summary, page 1-7
- Publishing Information, page 1-8
- Global vs. Local Administration Settings, page 1-9

What Is Cisco NAC Appliance?

The Cisco Network Admission Control (NAC) Appliance (formerly known as Cisco Clean Access) is a powerful, easy-to-use admission control and compliance enforcement solution. With comprehensive security features, in-band or out-of-band deployment options, user authentication tools, and bandwidth and traffic filtering controls, Cisco NAC Appliance is a complete solution for controlling and securing networks. As the central access management point for your network, Cisco NAC Appliance lets you implement security, access, and compliance policies in one place instead of having to propagate the policies throughout the network on many devices.

The security features in Cisco NAC Appliance include user authentication, policy-based traffic filtering, and client posture assessment and remediation. Clean Access stops viruses and worms at the edge of the network. With remote or local system checking, Clean Access lets you block user devices from accessing your network unless they meet the requirements you establish.

Cisco NAC Appliance is a network-centric integrated solution administered from the web console of the Clean Access Manager (CAM) administration server and enforced through the Clean Access Server (CAS) and (optionally) the Agent. You can deploy the Cisco NAC Appliance in the configuration that best meets the needs of your network. The Clean Access Server can be deployed as the first-hop gateway for your edge devices providing simple routing functionality, advanced DHCP services, and other services. Alternatively, if elements in your network already provide these services, the CAS can work alongside those elements without requiring changes to your existing network by being deployed as a “bump-in-the-wire.”
Cisco NAC Appliance Components

Other key features of Cisco NAC Appliance include:

- **Standards-based architecture**—Uses HTTP, HTTPS, XML, and Java Management Extensions (JMX).
- **User authentication**—Integrates with existing back end authentication servers, including Kerberos, LDAP, RADIUS, and Windows NT domain.
- **VPN concentrator integration**—Integrates with Cisco VPN concentrators (e.g. VPN 3000, ASA) and provides Single Sign-On (SSO).
- **Cisco NAC Appliance compliance policies**—Allows you to configure client posture assessment and remediation via use of Cisco NAC Appliance Agents or Nessus-based network port scanning.
- **L2 or L3 deployment options**—The Clean Access Server can be deployed within L2 proximity of users, or multiple hops away from users. You can use a single CAS for both L3 and L2 users.
- **In-Band (IB) or Out-of-Band (OOB) deployment options**—Cisco NAC Appliance can be deployed in-line with user traffic, or out-of-band to allow clients to traverse the network only during posture assessment and remediation while bypassing it after certification.
- **Traffic filtering policies**—Role-based IP and host-based policies provide fine-grained and flexible control for in-band network traffic.
- **Bandwidth management controls**—Limit bandwidth for downloads or uploads.
- **High availability**—Active/Passive failover (requiring two servers) ensures services continue if an unexpected shutdown occurs. You can configure pairs of Clean Access Manager (CAM) servers and/or CAS servers in high-availability mode.

Note: Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

Cisco NAC Appliance Components

Cisco NAC Appliance is a network-centric integrated solution administered from the Clean Access Manager web console and enforced through the Clean Access Server and (optionally) the Agent. Cisco NAC Appliance checks client systems, enforces network requirements, distributes patches and antivirus software, and quarantines vulnerable or infected clients for remediation before clients access the network. Cisco NAC Appliance consists of the following components (in Figure 1-1):

- **Clean Access Manager (CAM)**—Administration server for Cisco NAC Appliance deployment. The secure web console of the Clean Access Manager is the single point of management for up to 20 Clean Access Servers in a deployment (or 40 CASs if installing a SuperCAM). For Out-of-Band (OOB) deployment, the web admin console allows you to control switches and VLAN assignment of user ports through the use of SNMP.

  Note: The CAM web admin console supports Internet Explorer 6.0 or above only, and requires high encryption (64-bit or 128-bit). High encryption is also required for client browsers for web login and Agent authentication.

- **Clean Access Server (CAS)**—Enforcement server between the untrusted (managed) network and the trusted network. The CAS enforces the policies you have defined in the CAM web admin console, including network access privileges, authentication requirements, bandwidth restrictions, and Cisco NAC Appliance system requirements.
You can install a CAS as either a stand-alone appliance (like the Cisco NAC-3300 series) or as a network module (Cisco NME-NAC-K9) in a Cisco ISR chassis and deploy it In-Band (always inline with user traffic) or Out-of-Band (inline with user traffic only during authentication/posture assessment). The CAS can also be deployed in Layer 2 mode (users are L2-adjacent to CAS) or Layer 3 mode (users are multiple L3 hops away from the CAS).

You can also deploy several CASs of varying size/capacity to fit the needs of varying network segments. You can install Cisco NAC-3300 series appliances in your company headquarters core, for example, to handle thousands of users and simultaneously install one or more Cisco NAC network modules in ISR platforms to accommodate smaller groups of users at a satellite office, for example.

- **Cisco NAC Appliance Agents**—Optional read-only persistent or temporal Agents that reside on client machines. Cisco NAC Appliance Agent check applications, files, services, or registry keys to ensure that client machines meet your specified network and software requirements prior to gaining access to the network.

  Note  
  There is no client firewall restriction with client posture assessment via the Agent. The Agent can check the client registry, services, and applications even if a personal firewall is installed and running.

- **Cisco NAC Appliance Updates**—Regular updates of pre-packaged policies/rules that can be used to check the up-to-date status of operating systems, antivirus (AV), antispyware (AS), and other client software. Provides built-in support for AV vendors and AS vendors.
Clean Access Manager (CAM)

The Clean Access Manager (CAM) is the administration server and database which centralizes configuration and monitoring of all Clean Access Servers, users, and policies in a Cisco NAC Appliance deployment. You can use it to manage up to 20 Clean Access Servers. The web admin console for the Clean Access Manager is a secure, browser-based management interface (Figure 1-2). See “Admin Console Summary” in the Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(3) for a brief introduction to the modules of the web console. For out-of-band (OOB) deployment, the web admin console provides the OOB Management module to add and control switches in the Clean Access Manager’s domain and configure switch ports.
Clean Access Server (CAS)

The Clean Access Server (CAS) is the gateway between an untrusted and trusted network. The Clean Access Server can operate in one of the following In-Band (IB) or Out-of-Band (OOB) modes:

- IB Virtual Gateway (L2 transparent bridge mode)
- IB Real-IP Gateway
- OOB Virtual Gateway
- OOB Real-IP Gateway

The *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(3)* describes the global configuration and administration of Clean Access Servers and Cisco NAC Appliance deployment using the Clean Access Manager web admin console.

Cisco NAC Appliance Agents

When enabled for your Cisco NAC Appliance deployment, the Agent can ensure that computers accessing your network meet the system requirements you specify. The Agent is a read-only, easy-to-use, small-footprint program that resides on Windows user machines. When a user attempts to access the network, the Agent checks the client system for the software you require, and helps users acquire any missing updates or software.
Agent users who fail the system checks you have configured are assigned to the Agent Temporary role. This role gives users limited network access to access the resources needed to comply with the Agent requirements. Once a client system meets the requirements, it is considered “clean” and allowed network access.

The Cisco NAC Appliance Agent types available in Cisco NAC Appliance are:

- Cisco NAC Agent (persistent Agent for Windows client machines)
- Windows Clean Access Agent (persistent Agent for Windows client machines available prior to release 4.6(1) with which release 4.7 is backward compatible)
- Mac OS X Clean Access Agent (persistent Agent for Macintosh client machines)
- Cisco NAC Web Agent (temporal Agent for Windows client machines)

For more information on the Agent types available in Cisco NAC Appliance, see the “Cisco NAC Appliance Agents” chapter in the Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(3).

Cisco NAC Appliance Updates

Regular updates of pre-packaged policies/rules can be used to check the up-to-date status of operating systems, antivirus/antispyware software, and other client software. Cisco NAC Appliance provides built-in support for major AV and AS vendors. For more information, see the “Retrieving Cisco NAC Appliance Updates” section in the Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(3).

Clean Access Server Features

The following are key features and benefits of the Clean Access Server:

- In-Band or Out-of-Band deployment
- Layer 2 or Layer 3 deployment
- Integration with Cisco VPN concentrators
- Secure user authentication
- Cisco NAC Appliance network-based and Agent-based scanning and remediation
- Role-based access control
- DHCP address allocation for untrusted (managed) clients, or DHCP relay or passthrough modes
- Network address translation (NAT) services, with support for dynamic or 1:1 NAT (non-production only)
- Bandwidth management
- Event logging and reporting services
- VLAN support in which the Clean Access Server can be a VLAN termination point, provide VLAN passthrough, and provide VLAN-based access control.
- Flexible deployment options enabling the Clean Access Server to be integrated into most network architectures
• High availability—Active/Passive failover (requiring two servers) that ensures services continue if an unexpected shutdown occurs. You can configure pairs of Clean Access Manager (CAM) servers and/or CAS servers in high-availability mode.

Note: Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

CAS Management Pages Summary

A Clean Access Server must be added to the Clean Access Manager domain before it can be managed from the web admin console, as described in Add the CAS to the CAM, page 4-1. Once you have added the Clean Access Server, you access it from the admin console as shown in the following steps. In this document, CAS management pages refers to the set of pages, tabs, and forms accessed as shown below.

1. Click the CCA Servers link in the Device Management module. The List of Servers tab appears by default.

2. Click the Manage button for the Clean Access Server you want to access.

Note: For high-availability Clean Access Servers, the Service IP is automatically listed first, and the IP address of the currently active CAS is shown in brackets.

3. The CAS management pages are shown in Figure 1-4. The Status tab of appears by default.
The Clean Access Manager publishes the configuration settings to the Clean Access Servers whenever the following scenarios happen:

- A new CAS is added to the CAM.
- Connection between CAM and CAS restores after a communication failure between them.
- CAM boots up.
- CAS boots up.
- When CAM failover happens, the newly Active CAM would publish configuration to all connected CASs.
Global vs. Local Administration Settings

The Clean Access Manager web admin console has the following types of settings:

- **Clean Access Manager administration settings** are relevant only to the Clean Access Manager. These include its IP address and host name, SSL certificate information, and High-Availability (failover) settings.

- **Global administration settings** are set from the Clean Access Manager and applied to all Clean Access Servers. These include authentication server information, global device/subnet filter policies, user roles, and Cisco NAC Appliance configuration.

- **Local administration settings** are set in the CAS management pages of the admin console and apply only to that Clean Access Server. These include CAS network settings, SSL certificates, VPN concentrator integration, DHCP and 1:1 NAT configuration, IPSec key changes, local traffic control policies, and local device/subnet filter policies.

The global or local scope of a setting is indicated in the **Clean Access Server** column in the web admin console, as shown in Figure 1-5.

**Figure 1-5 Scope of Settings**

- **GLOBAL**—The entry was created using a global form in the CAM web admin console and applies to all Clean Access Servers in the CAM’s domain.

- **<IP Address>**—The entry was created using a local form from the CAS management pages and applies only for the Clean Access Server with this IP address.

In most cases, global settings are added, edited, and deleted from the global forms used to create them, and local settings are added, edited, and deleted from the local forms used to create them.

Some pages may display global settings (referenced by GLOBAL) and local settings (referenced by IP address) for convenience. Usually, the local settings may be edited or deleted from the global pages but can be **added** only from the local CAS management pages for a particular CAS.

**Priority of Settings**

Global (defined in CAM for all CASs) and local (CAS-specific) settings often coexist on the same CAS. If a global and local setting conflict, the local setting typically overrides the global setting. Note the following:

- For device filter policies affecting a range of MAC addresses and traffic control policies, the priority of the policy (higher or lower in **Device Management > Filters > Devices > Order**) determines which global or local policy to enforce. Any device filter policy for an individual MAC address takes precedence over a filter policy (either global or local) for a range of addresses that includes the individual MAC address.
• For subnet filter policies where one subnet filter specifies a subset of an address range in a broader subnet filter, the CAM determines the priority of the filter based on the size of the subnet address range. The smaller the subnet (like a /30 or /28 subnet mask), the higher the priority in the subnet filter hierarchy.

• Some features must be enabled on the CAS first (via the CAS management pages) before being configured in the CAM, for example:
  – Layer 3 support for the Agent (for multi-hop Layer 3 deployments)
  – Bandwidth Management
  – Use of VPN policy between CAS and users in user role

• Cisco NAC Appliance requirements and network scanning plugins are configured globally from the CAM and apply to all CASs.