Cisco NAC Appliance

Cisco® Network Admission Control (NAC) solutions allow you to authenticate wired, wireless, and VPN users and devices to the network; evaluate and remediate a device for policy compliance before permitting access to the network; differentiate access based on roles; and audit and report on who is on the network.

Product Overview

The Cisco NAC Appliance is a powerful, easy-to-deploy admission control and compliance enforcement component of the Cisco TrustSec™ solution. With comprehensive security features, in-band or out-of-band deployment options, user authentication tools, and bandwidth and traffic filtering controls, the Cisco NAC Appliance is a comprehensive solution for controlling and securing networks. You can implement security, access, and compliance policies through a central management point rather than configure policies throughout the network on individual devices.

Features and Benefits

The Cisco NAC Appliance is an integral component of the Cisco TrustSec solution. The Cisco NAC Appliance:

- Prevents unauthorized network access to protect your information assets
- Helps proactively mitigate network threats such as viruses, worms, and spyware
- Addresses vulnerabilities on user machines through periodic evaluation and remediation
- Brings you significant cost savings by automatically tracking, repairing, and updating client machines
- Recognizes and categorizes users and their devices before malicious code can cause damage
- Evaluates security policy compliance based on user type, device type, and operating system
- Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention
- Applies posture assessment and remediation services to a variety of devices, operating systems, and device access methods including LAN, WLAN, WAN, and VPN
- Enforces policies for all operating scenarios without requiring separate products or additional modules
- Supports seamless single sign-on through an agent with automated remediation
- Provides clientless web authentication for guest users

Authentication Integration with Single Sign-On

Cisco NAC works with existing authentication sources, natively integrating with Active Directory, Lightweight Directory Access Protocol (LDAP), RADIUS, Kerberos, S/Ident, and others. For the convenience of end users, Cisco NAC supports single sign-on for VPN clients, wireless clients, and Windows Active Directory domains. Administrators can maintain multiple user profiles with different permission levels through the use of role-based access control.

Device Quarantine

Cisco NAC can place noncompliant machines into quarantine, preventing the spread of infection while giving the machines access to remediation resources. Quarantine can be accomplished by using DHCP, inline traffic filters, or a quarantine VLAN.

Automatic Security Policy Updates

Automatic updates in Cisco's standard software maintenance package provide predefined policies for common network access criteria. These include policies that check for critical operating system updates, virus definition updates for antivirus software, and antispyware definition updates. This eases the management cost for network administrators, who can rely on Cisco NAC for constantly updated policies.

Centralized Management

The Cisco NAC web-based management console allows you to define a policy for the entire network, as well as the related remediation packages necessary for recovery. The management console manages the Cisco NAC Servers and network switches from a central interface.

Remediation and Repair

Quarantining allows remediation servers to provide operating system patches and updates, virus definition files, or endpoint security solutions to compromised or vulnerable devices. You can enable automated remediation through the optional agent, or specify your own remediation instructions. And Cisco NAC delivers user-friendly features, such as monitoring mode and silent remediation, to minimize user impact.

Flexible Deployment Modes

Cisco NAC offers the right deployment mode to fit your network. The appliance can be deployed in an in-band or out-of-band configuration. It can be deployed as a Layer 2 bridge and as a Layer 3 router. You can deploy it adjacent to the client on the same subnet or multiple router hops away.

Product Architecture

The Cisco NAC solution is comprised of the following components.

- **Cisco NAC Server:** The NAC Server enforces access privileges based on endpoint compliance and user authentication. A user cannot gain access to the network until they authenticate and the device meets defined posture requirements. The Cisco NAC Server is available in sizes for 100, 250, 500, 1500, 2500, 3500, and 5000 concurrent online users. The NAC Server is available as a standalone appliance and as a Network Module for Cisco routers. Appliances are available in different sizes and different software licenses.
- **Cisco NAC Manager:** This centralized, web-based console for establishing roles, checks, rules, and policies is available in three sizes. The Cisco NAC Lite Manager manages up to 3 Cisco NAC Servers; the Cisco NAC Standard Manager manages up to 20 Cisco NAC Servers; and the Cisco NAC Super Manager manages up to 40 Cisco NAC Servers or 80 Cisco NAC Network Modules. A single Cisco NAC Appliance Manager can manage up to 50,000 endpoints.
- **Cisco NAC Agent:** This thin, read-only agent enhances posture assessment functions and streamlines remediation. Cisco NAC Agents are optional and are distributed free of charge.

Additional NAC Services

The Cisco NAC Appliance Manager can be optionally deployed with the Cisco Identity Services Engine to provide Profiling services and with NAC Guest Server.

- **Cisco ISE (For Profiler):** Cisco ISE provides profiling capabilities that can analyze, discover and classify in real time all the endpoints connecting to the network. Cisco ISE comes with hundreds of built-in profiles for devices such as IP Phones, Printers, Mobile Devices (IPads, IPhones), Scanners etc, that make it possible to identify the type of device connecting to the network. Cisco ISE provides full visibility to an administrator of everything connected to the network in real time, and allows the administrator to control the access privileges associated with each type of endpoint.

  Cisco ISE 1.0MR can integrate with NAC Appliance 4.9 to provide Profiler capabilities to a NAC deployment. This combination of a Cisco NAC 4.9 Appliance deployment with an ISE 1.0MR deployment is the replacement for the Cisco NAC Profiler which is EoL.

  To find out more about Cisco ISE, please refer to the Data Sheet, at, http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11637/ps11195/data_sheet_c78-656174.html.
- **Cisco NAC Guest Server:** The optional Cisco NAC Guest Server simplifies the provisioning, notification, management, and reporting of guest users on wired and wireless networks. It can offload from IT staff many of the challenges of supporting corporate visitors. The Secure Guest service enhances your ability to protect your assets, employees, and information while providing network access that fully meets your visitors' business needs. For the Cisco NAC Guest Server data sheet, see http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/product_data_sheet0900aecd806e98c9.html.

In addition to the traffic flow modes, you have several other deployment options to best fit NAC into your network (see Table 1).

Table 1. Cisco NAC Network Module Deployment Options

Deployment Model	Options
Passing traffic mode	• Virtual gateway (bridged mode) • Real IP gateway (routed mode)
Client access mode	• Layer 2 (client is adjacent to the Cisco NAC Server) • Layer 3 (client is multiple hops from the Cisco NAC Server)
Traffic flow model	• In-band (Cisco NAC Server is always in line with user traffic) • Out-of-band (Cisco NAC Server is in line only during authentication, posture assessment, and remediation)

The Cisco NAC in-band mode supports any network infrastructure, and the out-of-band mode communicates with switches using Simple Network Management Protocol (SNMP). Please visit http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/switch_spt.html for the most recent list of supported switches.

Product Specifications

There are three hardware options for the NAC Server and NAC Manager (see Table 2).

Table 2. Cisco NAC Hardware Specifications

	Cisco NAC Appliance 3315	Cisco NAC Appliance 3355	Cisco NAC Appliance 3395
Product	• Cisco NAC Server for 100, 250, and 500 users • Cisco NAC Lite Manager	• Cisco NAC Server for 1500, 2500, 3500, and 5000 users • Cisco NAC Standard Manager	Cisco NAC Super Manager
Processor	1 x QuadCore Intel Core 2 CPU Q9400 @ 2.66 GHz	1 x QuadCore Intel Xeon CPU E5504 @ 2.00 GHz	2 x QuadCore Intel Xeon CPU E5504 @ 2.00 GHz
Memory	4 GB	4 GB	4 GB
Hard disk	2 x 250-GB SATA HDD	2 x 300-GB SAS RAID drives	4 x 300-GB SFF SAS RAID drives
Removable media	CD/DVD-ROM drive	CD/DVD-ROM drive	CD/DVD-ROM drive
Network Connectivity			
Ethernet NICs	• 2 x Integrated NICs • 2 x Integrated Gigabit NICs (PCI-X)	• 2 x Integrated NICs • 2 x Gigabit NICs (PCI-X)	• 2 x Integrated NICs • 2 x Gigabit NICs (PCI-X)
10BASE-T cable support	Cat 3, 4, or 5 unshielded twisted pair (UTP) up to 328 ft (100 m)	Cat 3, 4, or 5 UTP up to 328 ft (100 m)	Cat 3, 4, or 5 UTP up to 328 ft (100 m)
10/100/1000BASE-TX cable support	Cat 5 UTP up to 328 ft (100 m)	Cat 5 UTP up to 328 ft (100 m)	Cat 5 UTP up to 328 ft (100 m)
Secure Sockets Layer (SSL) accelerator card	None	Cavium CN1120-NHB-E	Cavium CN1120-NHB-E
Interfaces			
Serial ports	1	1	1
USB 2.0 ports	4 (two front, two rear)	4 (one front, one internal, two rear)	4 (one front, one internal, two rear)
Keyboard ports	1	1	1
Video ports	1	1	1
Mouse ports	1	1	1
External SCSI ports	None	None	None
System Unit			
Form factor	Rack-mount 1 RU	Rack-mount 1 RU	Rack-mount 1 RU
Weight	28 lb (12.7 kg) fully configured	35 lb (15.87 kg) fully configured	35 lb (15.87 kg) fully configured
Dimensions	Height: 1.69 in. (43 mm) Width: 17.32 in. (440 mm) Depth: 22 in. (559 mm)	Height: 1.69 in. (43 mm) Width: 17.32 in. (440 mm) Depth: 27.99 in. (711 mm)	Height: 1.69 in. (43 mm) Width: 17.32 in. (440 mm) Depth: 27.99 in. (711 mm)
Power supply	350W	Dual 675W (redundant)	Dual 675W (redundant)
Cooling fans	6; non-hot plug, nonredundant	9; redundant	9; redundant
BTU rating	1024 BTU/Hr (at 300W)	2661 BTU/Hr (at 120V)	2661 BTU/Hr (at 120V)
Regulatory and Standards Compliance			
Industry certifications	Criteria EAL2	Criteria EAL2	Criteria EAL2

System Requirements

The optional Cisco NAC Agent works on systems with the characteristics listed in Table 3.

Table 3. Cisco NAC Agent System Requirements

Feature	Minimum Requirement
Supported OS	Microsoft Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise, Windows Vista Home, Windows 7, Windows XP Professional, Windows XP Home, Windows XP Media Center Edition, Windows XP Tablet PC, Windows 2000, Windows 98, Windows SE, Windows ME, Mac OS X (v10.5.x, v10.6.x)
Hard drive space	Minimum of 10 MB free hard drive space
Hardware	No minimum hardware requirements (works on various client machines)

Cisco NAC also supports single sign-on for wireless and remote-access users using certain IP Security (IPSsec) VPN and WebVPN clients (see Table 4).

Table 4. VPN and Wireless Components Supported with Single Sign-On

Product	Clients
Cisco wireless LAN controllers	-
Cisco ASA 5500 Series Adaptive Security Appliances	• Cisco SSL VPN (tunnel) • Cisco IPsec VPN Client
Cisco WebVPN Service Modules for Cisco Catalyst® 6500 Series Switches and Cisco 7600 Series Routers	
Cisco VPN 3000 Series Concentrators	
Cisco PIX® Security Appliances	

Cisco NAC is preconfigured to offer policy checks for more than 350 applications from 50 vendors. This list is constantly being expanded; visit http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html for the latest supported applications (listed under “Cisco NAC Appliance Supported AV/AS Product List”).

Note: Not all check types are supported for all products, and some vendors do not support Windows 9x. In addition to the preconfigured checks, you have full access to the Cisco NAC rules engine and can create any custom check or rule for any other third-party application.

Service and Support

Cisco offers a wide range of services programs to accelerate your success. These innovative programs are delivered through a combination of people, processes, tools, and partners that results in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, see Cisco Technical Support Services or Cisco Advanced Services.

Warranty information is available at http://www.cisco.com/go/warranty. Licensing information is available at http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/license.html.

For More Information

For more information about Cisco NAC products and the Cisco TrustSec solution, visit http://www.cisco.com/go/nacappliance or contact your local Cisco account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C78-562875-04 09/11