



SOLUTION OVERVIEW

NETWORK ADMISSION CONTROL COLLABORATION— CISCO SYSTEMS AND SYMANTEC



Organizations depend on their networks to be reliable and available at all times in order to communicate with customers and partners, to provide customer support, and to execute business transactions. To provide these services on an ongoing basis, organizations must enable access to the network through entry points such as VPNs, intranets, and extranets, from a growing number of endpoints, including laptops, desktops, and mobile devices. In this 24x7 business environment, network downtime can cost millions of dollars in lost revenue and productivity. It is essential for organizations to protect their network assets and mission-critical applications from hackers, worms, viruses, and more—a task that becomes ever more difficult in today's always-on, always-connected business environment.

MAXIMUM NETWORK SECURITY STARTS AT THE ENDPOINT

To address challenges created by the growing variety of endpoints, and to maximize the overall security posture of the network, infrastructure and security providers have recognized the need for interoperable solutions that enforce security policies at every endpoint.

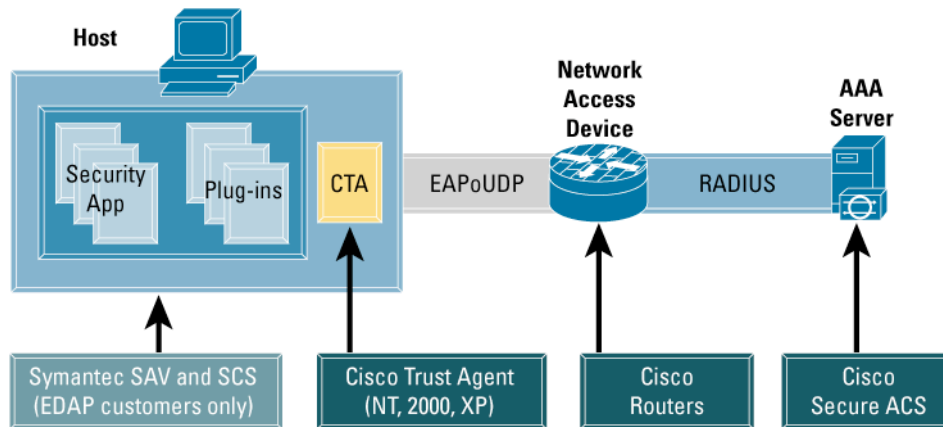
In November 2003, Symantec and Cisco Systems® announced Network Admission Control (NAC), a multi-vendor, industry-wide collaboration, led by Cisco, focused on minimizing the damage organizations face from emerging security threats. Cisco is the worldwide leader in networking and the founder of the Self-Defending Network strategy. Symantec is the leader in Internet security. The two companies have worked together to ensure product interoperability and address endpoint security issues and policy enforcement.

Through NAC Program interoperability efforts, Symantec Client Security and Symantec AntiVirus Corporate Edition products now work with the Cisco Trust Agent to provide the ability to enforce access privileges on the endpoint (see systems requirements below).

How Cisco—Symantec NAC works can be best illustrated by the five components in Figure 1, “Cisco—Symantec NAC Process”:

- 1. Endpoint security solutions**—The Symantec Client Security and Symantec AntiVirus Corporate Edition products deliver industry-leading endpoint protection.
- 2. Communications agent**—Symantec endpoint security solutions interact with the Cisco Trust Agent, a software application that resides on the endpoint, collects security state information from the Symantec client, and communicates it to the Cisco network access device.
- 3. Network access device**—Every endpoint device seeking access to the network contacts a router, switch, VPN concentrator, firewall, or other network access device. The network access device requests security credentials from the endpoint device, through the Cisco Trust Agent, regarding the state of the endpoint device security, including the Symantec security solutions. This information is then relayed to the Cisco Secure Access Control Server (ACS).
- 4. Policy server**—Cisco Secure ACS evaluates endpoint security credentials and determines the appropriate policy—permit, deny, quarantine or restrict access. The policy is then enforced by the Cisco network access device.
- 5. Centralized management system**—The CiscoWorks VPN/Security Management Solution, CiscoWorks Security Information Manager Solution (SIMS), and Symantec Security Management System solution provision NAC elements, to provide monitoring and reporting tools, and to enable the management of endpoint security applications.

Figure 1. Symantec NAC Process



MAXIMUM BUSINESS BENEFITS

Symantec's participation in the NAC program allows enterprises to use existing corporate investments in both security software and network infrastructure to strengthen security policies and enforce compliance. Additionally, it allows organizations to proactively minimize network downtime and protect network availability and integrity from external and internal threats. By enabling security policy enforcement and access management at network endpoints, organizations the power to:

- Reduce IT costs and total cost of ownership
- Maintain the productivity of IT personnel, enabling them to focus on higher-value initiatives
- Minimize risk by helping to ensure that all devices comply with corporate security policies
- Prevent endpoints from infecting the corporate network with harmful worms and viruses
- Maximize existing Symantec and Cisco investments
- Increase network availability, resilience, and productivity

A PHASED APPROACH

Collaboration efforts to date reflect what Cisco and Symantec call Phase One NAC integration. Phase One interoperability includes Symantec AntiVirus Corporate Edition 9.0 or Symantec Client Security 2.0 with the Cisco Trust Agent 1.0 (see systems requirements below), and helps ensure that Symantec software is installed, running, and versioned appropriately, before allowing endpoint connectivity to the network.

Other Cisco products included in Phase One are access and midrange routers, including current Cisco 1700 to 7200 series routers. Symantec's Phase One release is available to its EDAP customers of Symantec AntiVirus Corporate Edition 9.0 and Symantec Client Security 2.0. Symantec will make Phase One generally available to its customers in a future release.

In Phase Two, Cisco will expand NAC support to Cisco Catalyst® switches and VPN 3000 Series concentrators, will increase the number of supported applications through an API, and will increase the number of supported endpoint operating systems. Cisco will also improve handling for endpoints, such as printers, unable to communicate with systems enforcing network admission. Subsequent NAC phases will extend platform support to all network access devices, including firewalls and wireless access points.

PROTECTION FROM LEADERS IN THE INDUSTRY

As the leader in Internet security, Symantec has an exceptionally strong track record of integrating leading-edge security software technologies. The company's expertise in identifying known and unknown threats and vulnerabilities in endpoint systems, plus its ability to meet the challenge of blended threats by using coordinated security technologies, makes Symantec ideally suited for participation in the NAC program.

Cisco is the worldwide leader in networking for the Internet. The NAC program is part of the Cisco Self-Defending Network strategy to increase the network's ability to identify, prevent, and adapt to threats.

AN INTEGRATED SOLUTION FROM THE BIGGEST NAMES IN THE BUSINESS

Unlike standalone security products, the offerings from Symantec and Cisco provide customers admission control coverage in its network, along with central management options that increase flexibility without compromising protection. As industry leaders, Symantec and Cisco have joined forces to help mutual customers proactively mitigate risks by identifying, preventing, and adapting to new and emerging security threats.

SYSTEM REQUIREMENTS, PHASE ONE

Cisco

- Cisco Trust Agent 1.0 (Windows NT, 2000, XP)
- Cisco 83XX to 72XX routers running Cisco IOS® Software Release 12.3(8)T with security
- Cisco Secure ACS Version 3.3
- CiscoWorks SIMS Version 3.1.2

Symantec

- Symantec Client Security 2.0
- Symantec AntiVirus Corporate Edition 9.0
- Symantec Posture Plugin for Cisco Trust Agent.

Next Steps

For more information about the Symantec and Cisco collaboration in NAC, visit: <http://www.cisco.com/go/nac> or e-mail: Sym_NAC@symantec.com



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, Cisco Systems logo, are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Copyright © 2004 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holder/s. All product information is subject to change without notice.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R) 204107_ETMG_Rdlc_11.04

