



Release Notes for Network Admission Control, Release 1.0

Contents

- [Introduction](#)
- [NAC Overview](#)
- [IOS](#)
- [Cisco Trust Agent \(CTA\)](#)
- [Cisco Access Control Server \(ACS\)](#)
- [CiscoWorks SIMS](#)
- [Cisco Security Agent \(CSA\)](#)
- [System Caveats and Performance](#)
- [Additional Information](#)
- [Software Version Matrix](#)
- [Cisco NAC Platform Support](#)

Introduction

The following release notes apply to Network Admission Control (NAC), Release 1.0 (formerly referred to as Phase One or Phase 1 Solution). NAC was released in June, 2004.

Document Purpose

This document describes the limitations of Network Admission Control, Release 1.0. For detailed release notes about the individual NAC components, refer to the links in [Table 1](#).



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

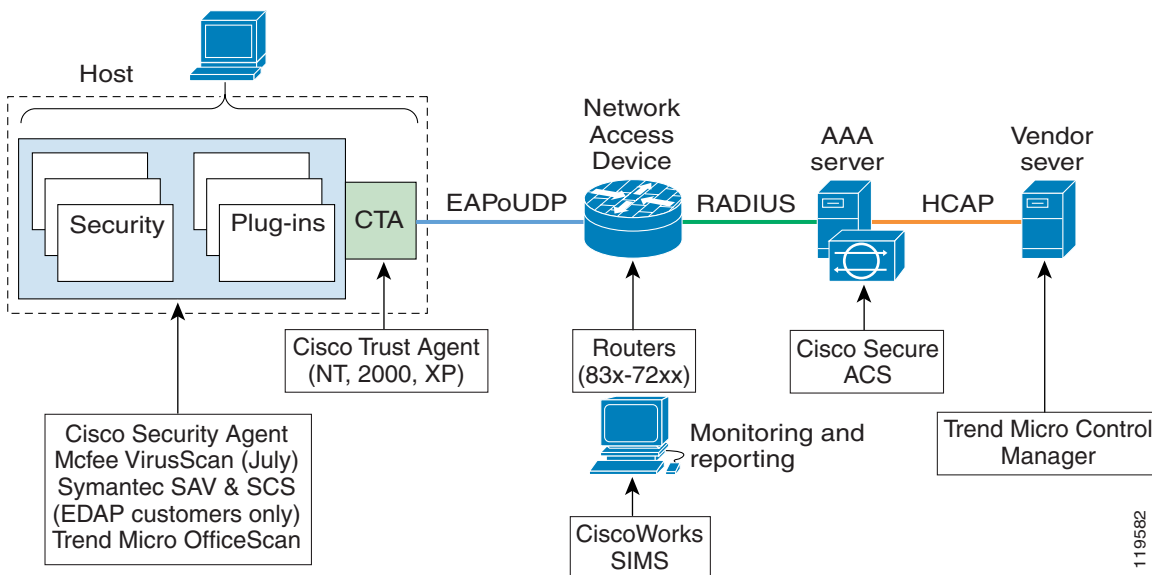
Audience

The target audience for this document is the system engineers and network administrators responsible for the implementation of Network Admission Control (NAC).

NAC Overview

Virus infection on data networks has become an increasingly serious problem. The resources consumed during just one disinfection process are much greater than the resources necessary to implement an anti-virus feature in the network such as Network Admission Control. Cisco's Network Admission Control (NAC) is such a feature and is deployed to ensure the health of all client workstations prior to those workstations being granted network access. NAC is a technology that works in conjunction with anti-virus vendor's software to assess the condition or "posture" of a client prior to granting network access. This ensures a workstation has an up-to-date virus signature set and has not been infected prior to gaining access to a data network. If the workstation requires a signature update an action is sent back to the workstation directing it to complete the update or, if the workstation has been compromised or a network outbreak has occurred, places it into a quarantined network segment until the update or disinfection process can be completed.

Figure 1 NAC Solution Architecture



IOS

Production Enhancements

While 12.3(8)T was released with NAC support in May, 2004 and is currently available, the first IOS rebuild (12.3(8)T.1) has several enhancements and is the version that customers should look at for production deployment.

Auth Proxy

See also the AAA Release Notes located at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfauthp.htm#1001143

Protection Against Denial-of-Service Attacks

NAC proxy monitors the level of incoming hosts.. For each request, NAC requests the host for posture information. A high number of open requests could indicate that the router is the subject of a denial-of-service (DoS) attack. The authentication proxy limits the level of open requests and drops additional requests until the number of open requests has fallen below 100.

If the router is experiencing a high level of host connection requests requiring posture validation, legitimate hosts may experience delays before posture validation completes.

Risk of Spoofing with NAC

When NAC succeeds, it creates a temporary dynamic access control entry for the host. While this entry exists, another host might spoof the validated host's address to gain access behind the router. NAC does not cause the address spoofing problem; the problem is only identified here as a matter of concern to the user. Spoofing is a problem inherent to all access lists, and NAC does not specifically address this problem.

NAT and NAC

Because EAPoUDP is initiated from a router rather than a host, NAT issues may arise where NAT is deployed between host and router. NAT implementations that depend on a host first having sent an EAPoUDP packet before forwarding an EAPoUDP request from the router are not supported.

However, NAC and NAT can co-exist on the same router.

PAT and NAC

NAC does not support deployments where PAT is enabled between host and the router.

Cisco Trust Agent (CTA)

There have been several minor improvements made to CTA. To take full advantage of these improvements, we strongly recommend that you use CTA version 1.0 or later for production deployments.

Cisco Access Control Server (ACS)

ACS version 3.3 is available on www.cisco.com for upgrades. Refer to [Table 1](#) for links to more information. The ACS Appliance is scheduled to be available in July, 2004.

CiscoWorks SIMS

Cisoworks SIMS version 3.1.2 is available on www.cisco.com for upgrades. Refer to [Table 1](#) for links to more information. The Cisoworks SIMS appliance is scheduled to be delivered at a later date.

Cisco Security Agent (CSA)

CSA can protect the other NAC components on the host (posture plug-ins and CTA) and requires a special configuration. Refer to [Table 1](#) for links to more information.

System Caveats and Performance

Language Support for Operating Systems

Currently the US English version of the supported Microsoft operating systems has been fully qualified¹. The following additional language versions of the supported Microsoft operating systems will be qualified in the Summer 2004 timeframe:

- UK
- French, Italian, German, Spanish
- Japanese
- Chinese
- Korean

Additional Information

Table 1 *Links to Code and Documentation*

1. Cisco intends to support (through TAC) CTA on any of the supported Microsoft operating systems, not just those that are qualified.

NAC Component	Code	User Documentation	Release Notes
Cisco Trust Agent (CTA)	http://www.cisco.com/cgi-bin/tablebuild.pl/cta	http://www.cisco.com/en/US/products/ps5923/products_administration_guide_book09186a008023f7a5.html	http://www.cisco.com/cgi-bin/tablebuild.pl/cta
IOS	http://www.cisco.com/public/sw-center/sw-ios.shtml	http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm	http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123t/index.htm
Access Control Server (ACS)	http://www.cisco.com/kobayashi/sw-center/ciscosecure/cs-acss.shtml	http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/	http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/
Ciscoworks SIMS	http://www.cisco.com/en/US/products/sw/cscowork/ps5209/ps5280/index.html	http://www.cisco.com/en/US/products/sw/cscowork/ps5209/ps5280/index.html	http://www.cisco.com/en/US/products/sw/cscowork/ps5209/ps5280/index.html
Solution		<i>Deploying Network Admission Control</i> http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd800fdd7b.pdf	This document represents the Release Notes for NAC, Release 1.0.

Software Version Matrix

Refer to the following table to find the system requirements for NAC.

Table 2 System Requirements

Component	Minimum Version
Cisco IOS	IOS (12.3(8)T) or later (recommend 12.3(8)T.1 or later)
Cisco Trust Agent	CTA 1.0 or later
Cisco Access Control Server	ACS 3.3 or later
Cisco Security Agent	CSA 4.0.2 or later
CiscoWorks NMS	CiscoWorks SIMS 3.1.2 or later
Trend Micro AV	Trend OfficeScan Enterprise 6.5

Component	Minimum Version
McAfee AV	McAfee VirusScan Enterprise 7.0, 7.1 and 8.0i
Symantec AV	Symantec AntiVirus 9.0 and SCS 2.0 (Enterprise Development Alliance Program only)

Cisco NAC Platform Support

Refer to [Table 3](#) to find the platforms supported by NAC. [Table 4](#) lists specific platforms that are not supported by the current solution.

Table 3 Supported Platforms

Supported Platform	Models	IOS Images
Cisco 7XXX	7200	IP IPSec 3DES IP FW/IDS IP FW/IDS IPSec 3DES Enterprise IPSec 3DES Enterprise FW/IDS Enterprise FW/IDS IPSec 3DES
Cisco 37XX	3745, 3725	Advanced Security Advanced Services Advanced Enterprise
Cisco 36XX	3640/3640A 3660-ENT Series	ENTERPRISE/FW/IDS PLUS IPSEC 3DES IP/FW/IDS IP/FW/IDS PLUS IPSEC 3DES IP/IPX/APPLETALK PLUS FW/IDS
Cisco 26XX	2600XM, 2691	Advanced Security Advanced Services Advanced Enterprise
Cisco 17XX	1701, 1711, 1712, 1721 1751, 1751-V, 1760	IP/ADSL/IPX/AT/IBM/VOX/FW/IDS Plus IPSec 3DES IP/ADSL/IPX/AT/IBM/FW/IDS Plus IPSec 3DES IP/ADSL/VOX/FW/IDS Plus IPSec 3DES IP/ADSL/FW/IDS PLUS IPSec 3DES Advanced Security Advanced Services Advanced Enterprise
Cisco 83x	831, 836, 837	IP/Firewall/IPSec 3DES PLUS IP/Firewall/IPSec 3DES/ PLUS/dial backup

Table 4 *Platforms Not Supported*

Platform	Unsupported Models
Cisco 17XX	1750, 1720, 1710
Cisco 26XX	2600 non-XM models
Cisco 36XX	3620, 3660-CO series

This document is to be used in conjunction with the documents listed in the [“Additional Information”](#) section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

