Cisco NAC Appliance Executive Overview
Contents

1 The “Business Case” For Network Admission Control
2 Cisco NAC Appliance Product Overview
3 Common NAC Posture Assessments
4 Deployment Considerations
5 Additional Resources
The Vulnerability of Networks

Every **bit** of user data touches the network

Every **device** employee, consultant and guest has is attached to the network

In this environment, **EVERYTHING** is a potential target AND a potential threat

**>>** Threat vectors have changed: your “trusted users” can be the weakest link in your network’s security
The Evolution of Threats

Mitigating threats via policy compliance

Balancing productivity and security in a “connected” world

Changing threats from data-in-transit to data-in-storage

>> Business vectors have changed: you are accountable for your “policies” that are not enforced
Common Ways to Combat Threats

1. Require users to abide by “responsible computing” guidelines
   **BUT** No direct pain, no responsibility

2. Register use computers; require authentication
   **BUT** Authentication not enough

3. Pass out anti-X software, OS updates through patch management systems
   **BUT** Compliance is still voluntary and unenforceable

4. Use IDS/IPS/endpoint monitoring solutions to find bad computers
   **BUT** Does not stop vulnerabilities and fails to fix problem
Make Access Contingent on Compliance

First, establish ACCESS POLICIES. Then:

Authenticate & Authorize
- Enforces authorization policies and privileges
- Supports multiple user roles

Scan & Evaluate
- Agent scan for required versions of hotfixes, AV, etc
- Network scan for virus and worm infections and port vulnerabilities

Quarantine & Enforce
- Isolate non-compliant devices from rest of network
- MAC and IP-based quarantine effective at a per-user level

Update & Remediate
- Network-based tools for vulnerability and threat remediation
- Help-desk integration

NO COMPLIANCE = NO NETWORK ACCESS
Contents

1. The “Business Case” For Network Admission Control
2. Cisco NAC Appliance Product Overview
3. Common NAC Posture Assessments
4. Deployment Considerations
5. Additional Resources
### NAC Means Better Criteria for Security

| What System Is It? | Windows, Mac or Linux  
|--------------------|------------------------|
|                    | Laptop or Desktop or PDA  
|                    | Printer or Other Corporate Asset  

| Who Owns It? | Company  
|--------------|------------------------|
|              | Employee  
|              | Contractor  
|              | Guest  
|              | Unknown  

| Where Is It Coming From? | VPN  
|--------------------------|------------------------|
|                          | LAN  
|                          | WLAN  
|                          | WAN  

| What’s On It? | Anti-Virus, Anti-Spyware  
|---------------|------------------------|
|               | Personal Firewall  
|               | Patching Tools  

| Is It Running? |  
|----------------|------------------------|

| What’s The Preferred Way To Check/Fix It? | Pre-Configured Checks  
|------------------------------------------|------------------------|
|                                          | Customized Checks  
|                                          | Self-Remediation or Auto-Remediation  
|                                          | Third-Party Software  

## Four Key Capabilities of Cisco NAC

<table>
<thead>
<tr>
<th>What It Means</th>
<th>Securely Identify Device and User</th>
<th>Enforce Consistent Policy</th>
<th>Quarantine and Remediate</th>
<th>Configure and Manage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate Users to Devices</td>
<td>Assess Devices; Enforce Policies</td>
<td>Isolate and Fix Non-compliant Devices</td>
<td>Create and Manage Policies Easily</td>
<td></td>
</tr>
</tbody>
</table>

### Why It Is Important

<table>
<thead>
<tr>
<th>Securely Identify Device and User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associating Users with Devices Enables Granular Enforcement of Policies by Role or group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enforce Consistent Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforcement at the Network Reduces Reliance on the Integrity of the Endpoint</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quarantine and Remediate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine Critical to Halt Spread of Vulnerabilities; Remediation Addresses Root Cost Drivers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configure and Manage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies That Are Easy to Create and Maintain Lead to Better System Operations and Adherence</td>
</tr>
</tbody>
</table>

### A Comprehensive NAC Solution Must Have All Four Capabilities: The Absence of Any One Weakens the Solution
Customer Pain Points

Top Customer Pain Points*

Role-based access control
Cisco NAC applies access and posture policies based on roles

Enforce endpoint policy requirements
Cisco NAC assesses, quarantines, and remediates noncompliant endpoints

Guests and unmanaged users
Cisco NAC authenticates and controls guest and unmanaged assets

* Source: Current Analysis, July 2006
Cisco NAC Is Widely Deployed Today

- Cisco NAC Appliance has 1200+ customers
- Mid-market and large enterprises
  - Financial services
  - Healthcare
  - Public sector
  - Manufacturing
- All use cases
  - Remote access
  - Guest users
  - Wireless
  - LAN/VoIP
Cisco NAC Appliance Advantage

1. One Product for All Use Cases

2. Number 1: Most amount of experience brings the most relevant features

3. Easy to own: Most deployments ready under five days

4. Scalable: Installations from 100 users to 100,000+ users, from single site to 150+ locations

5. Flexible: Does not require an infrastructure upgrade
NAC Appliance Components

- **Cisco Clean Access Manager**
  Centralizes management for administrators, support personnel, and operators

- **Cisco Clean Access Server**
  Serves as enforcement point for network access control

- **Cisco Clean Access Agent**
  Optional lightweight client for device-based registry scans in unmanaged environments

- **Rule-set Updates**
  Scheduled automatic updates for anti-virus, critical hot-fixes and other applications
NAC Appliance Sizing

Super Manager manages up to 40 Enterprise and Branch Servers

Standard Manager manages up to 20 Branch Office or SMB Servers

Manager Lite manages up to 3 Users = online, concurrent

100 users 250 users 500 users

1500 users each

2500 users each
NAC Appliance Use Cases

Wireless Compliance
Secured network access only for compliant wireless devices

Guest Compliance
Restricted internet access only for guest users

Endpoint Compliance
Network access only for compliant devices

Intranet Access Compliance
Ensure hosts are hardened prior to connecting to ERP, HRIS, BPM, etc.

VPN User Compliance
Intranet access only for compliant remote access users
Cisco NAC Appliance Overview

1. End user attempts to access a Web page or uses an optional client
   Network access is blocked until wired or wireless end user provides login information

2. User is redirected to a login page
   Clean Access validates username and password, also performs device and network scans to assess vulnerabilities on the device

3a. Device is noncompliant or login is incorrect
   User is denied access and assigned to a quarantine role with access to online remediation resources

3b. Device is “clean”
   Machine gets on “certified devices list” and is granted access to network
End User Experience: Web-based

Scan is performed
(types of checks depend on user role/OS)

Click-through remediation
End User Experience: with Agent

Login Screen

Scan is performed............
(types of checks depend on user role)

Scan fails

Remediate

You have temporary access!

Your system does not meet the requirements enforced by the network administrator. You may only have limited access to the network until your system meets all the requirements.

There is approximately 0:03:59 left before your temporary access expires.

Please click on "Continue" and follow the instructions to satisfy network access requirements.

Clean Access Agent

Required Software

Name: Anti-Spyware (Optional) Software
Version: 
Location: http://www.360safe.com/support/download/

Description: Our security policy recommends that you download an anti-spyware program. Click Go To Link to download a free Anti-Spyware program or click Next to skip.

Go To Link  Next  Cancel
Cisco NAC Appliance Partnerships

Cisco NAC is committed to protecting customer’s investments in partner applications

NAC Appliance Supports Policies for 250+ Applications, Including These Vendors:
Complementary Cisco Products

- **Switches and Routers**
  - All switches and routers (In Band)
  - Catalyst 2900, 2940/50/60, 3500, 3550/60, 3750, 4000/4500, 6500 (Out of Band)
- **Cisco Security Agent for day-zero endpoint security**
- **Cisco MARS for security correlation**
- **VPN products**
  - VPN3000 Concentrator
  - ASA/PIX70
  - ISR/IOS
  - WebVPN
- **Wireless APs**
  - WLSM (Aironet)
  - Wireless Controllers ( Airespace)
Contents

1  The “Business Case” For Network Admission Control
2  Cisco NAC Appliance Product Overview
3  Common NAC Posture Assessments
4  Deployment Considerations
5  Additional Resources
Corporate/Employee Posture Assessment

Corporate Asset Tag
- Unique registries inserted into corporate devices
- Corporate PKI certificates installed in corporate devices

Microsoft Hotfixes:
- Critical hot-fixes checks (provided via Cisco automated updates)
- SUS/WUS running or AU Options (can force setting)
- SMS or Patch Management SW running (can launch qualified .exe)

Security Applications:
- HIDS (CSA) or Personal Firewall installed and running
- AV installed, running and latest DAT (can launch AV)
- Anti-Spyware installed and running
- Encryption software installed and running
NAC Decision Tree for Employee

- Corp Asset Tag
- SUS/SMS/CSA
- Hotfixes
- AV/AS UptoDate
- No access, call HelpDesk
- No access, start service
- Internet only, launch AV
- Internet only, SUS/SMS runs
- Access

Quarantine
Contents

1 The “Business Case” For Network Admission Control
2 Cisco NAC Appliance Product Overview
3 Common NAC Posture Assessments
4 Deployment Considerations
5 Additional Resources
Cisco Clean Access for Corporate LAN

FEATURES
- Supports 802.1q trunking
- Supports both L3 multi-hop and L2
- Supports L2TPv3 tunneling
- Supports both inband and out-of-band

BENEFITS
- Enables central deployment mode
- End user devices can be several hops away
- Extends enforcement to campus buildings
Cisco Clean Access for Remote Users

**FEATURES**
- Supports IPSec and SSL Tunnel VPNs
- Supports site-to-site VPNs
- Supports VPN user sign-on

**BENEFITS**
- Extends policy enforcement and compliance to remote access and VPN users
- Extends enforcement to site-to-site VPN partners
- Leverages VPN sign-on for single-sign-on
Cisco Clean Access for Wireless Users

**Features**
- Supports 802.1q trunking
- Support L2TPv3 or GRE tunneling
- Supports thin or thick wireless 802.11 APs
- Supports Wireless user sign-on

**Benefits**
- Enables central deployment mode
- End user devices can be several hops away
- Extends enforcement to any wireless networks
- Leverages EAP sign-on for single-sign-on
ADDITIONAL RESOURCES

Product information at:
www.cisco.com/go/nac/appliance

Specific questions to:
cca-questions@cisco.com