Designing and Deploying Cisco NAC Appliance

Timothy Snow
Consulting System Engineer
tisnow@cisco.com

Cisco Networkers Solutions Forum 2007
Network Design and Deployment: Agenda

1. NAC Appliance Overview
2. Clean Access Server Foundation Concepts
3. Clean Access Server Deployment Examples
4. Clean Access Manager Options
5. Failover Configurations
Problem: Worms Still Cause Outages
Perimeter Security Is Not Enough

>> Threat vectors have changed: “friendly users” can be the weakest link in your network’s security

Complicated by:

User types: employees, contractors
guests, partners

Device types: laptops, PDAs, desktops
managed, unmanaged

Access types: remote/VPN, wireless
LAN, branch offices

Does each user have:
- [✓] Windows Updates?
- [✓] Anti-virus software?
- [✓] Anti-spyware software?
How Do You Guarantee Compliance?

1. Establish granular, specific access policies
   
   e.g. “All users entering in ‘employee_sales’ role must have Symantec AntiVirus version 9.x or greater!”

2. Recognize who (what type of user) and what (the device type) is connecting to the network

3. Evaluate all systems that connect to ensure that they are “clean”

4. Quarantine “unclean” systems until they are “cleaned”

5. Automate the process both from an evaluation and a remediation standpoint

NO COMPLIANCE = NO NETWORK ACCESS
Network Admission Control
“The Network Is The Control Point”

Apply **Network Admissions Control**, no matter:

- What system it is (printer, Windows PC, Mac laptop, Linux workstation)
- Where it’s coming from (VPN, LAN, WLAN, WAN)
- Who owns it (company, employee, contractor, guest, unknown)
- What applications are on the system (AV, personal firewall, patching tool)
- How it’s checked and fixed (pre-configured, customized, 3rd party)
NAC Appliance Overview

All-in-One Policy Compliance and Remediation Solution

**AUTHENTICATE & AUTHORIZE**
- Enforces authorization policies and privileges
- Supports multiple user roles

**SCAN & EVALUATE**
- Agent scan for required versions of hotfixes, AV, and other software
- Network scan for virus and worm infections and port vulnerabilities

**QUARANTINE**
- 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
NAC Appliance Overview: Components

- **Cisco Clean Access Server**
  Serves as an in-band or out-of-band device for network access control

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

- **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 Overview: Components

Critical Windows Updates
Windows XP, Windows 2000, Windows 98, Windows ME

Anti-Virus Updates

Anti-Spyware Updates
Other 3rd Party Checks

Customers can easily add customized checks
Note on Scaling Numbers

Values apply to concurrent users only, NOT concurrent devices. (User = something we have posture-assessed.)

Bandwidth is the least important calculation for determining how many users a CAS can handle.

Factors included are numerous:

- Number of new user authentications per second
- Number of posture assessments per second
- How many checks are in each posture assessment
- Number of agent-less network scans per second
- Number of plug-ins per scan
- Rescan timer intervals
- Per role and total online timer intervals
- Bandwidth controls
- Filters and access controls
NAC Appliance Overview: Solution Sizing

Super Manager manages up to 40 Enterprise and Branch Servers

Standard Manager manages up to 20 Enterprise and Branch Servers

Manager Lite manages up to 3 Enterprise and Branch Servers

Branch Office or SMB Servers
- 100 users
- 250 users
- 500 users

Users = online, concurrent

1500 users each
THE GOAL

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
   NAC Appliance 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
NAC Appliance Overview: Agent

Login Screen

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

Scan fails

Remediate
NAC Appliance Overview: Web Login

Login Screen

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

Click-through remediation

Note that all existing anti-virus software should be removed from your computer before installing the Anti-Virus software. For complete installation instructions, see the How-To document.

The ITS Support Center will be delighted to answer any questions you have about the procedure. Contact
NAC Appliance Overview: Process Flow

User Machine -> Server -> Manager

- UDP Discover (8905, 8906)
- DHCP Request
- URL Redirect to Weblogin
- Connect via TCP (443)
- Download Clean Access Agent
- Connect via TCP (443)
- Download Policy to Agent
- Agent Performs Posture Assessment
- Pre-connect (1099)
- Connect request (1099)
- Connect Response (8955, 8956)
- User Login (443)
- Agent download (80)
- Agent checks and rules, XML (443)
- Plugins enabled (443)
- Agent Performs Access Enforcement
- Certified and Logged On
- Logged out
- Report (443)
- Session and heartbeat timer (443)
Network Design and Deployment: Agenda

1. NAC Appliance Overview
2. Clean Access Server Foundation Concepts:
   - Virtual Gateway / Real IP Gateway
   - (L2/L3 device)
   - Central Deployment / Edge Deployment
   - Layer 2 / Layer 3
   - In Band / Out of Band
3. Clean Access Server Deployment Examples
4. Clean Access Manager Options
5. Failover Configurations
CAS Foundation: Virtual Gateway & Real IP Gateway

- Clean Access Servers at the most basic level can pass traffic in one of two ways:
  - Bridged Mode = Virtual Gateway (Frames)
  - Routed Mode = Real IP Gateway / NAT Gateway (Packets)

- Any CAS can be configured for either method, but a CAS can only be one at a time

- Gateway mode selection affects the logical traffic path

- Does not affect whether a CAS is in Layer 2 mode, Layer 3 mode, In Band or Out of Band
CAS Foundation: Virtual Gateway

- Direct Bridging: Frame Comes In, Frame Goes Out
- VLAN IDs are either passed through untouched or mapped from A to B
- DHCP and Client Routes point directly to network devices on the Trusted side
- CAS is an IP passive bump in the wire, like a transparent firewall
**CAS Foundation: Real IP / NAT Gateway**

- CAS is Routing, Packet Comes In, Packet Goes Out
- VLAN IDs terminate at the CAS, no pass-through or mapping
- DHCP and Client Routes usually point to the CAS for /30 – Handles broadcast domains
- CAS is an active IP router, can also NAT outbound packets **
CAS Foundation: Central & Edge Deployment

- Clean Access Servers have two physical deployment models
  - Edge Deployment (Uplink based – Unlikely)
  - Central Deployment (Likely)
- Any CAS can be configured for either method
- Deployment mode selection affects the physical traffic path
- Does not affect whether a CAS is in Layer 2 mode, Layer 3 mode, In Band or Out of Band
CAS Foundation: Edge Deployment

- Easiest deployment option to understand
- CAS is logically inline, and physically inline
- Supports all Catalyst Switches
- VLAN IDs are passed straight through when in VGW
  \[10 \rightarrow 10\]
- Installations with multiple Access Layer closets can become complex
CAS Foundation: Central Deployment

- Most common deployment option
- CAS is logically inline, NOT physically inline
- Supports 6500 / 4500 / 3750 / 3560 **
- VLAN IDs are mapped when in VGW
  
  110 → 10
- Easiest installation
- Most scalable in large environments
CAS Foundation: Central Deployment

Example Enterprise Central Deployment

Virtual Gateway Mode

- 3 Access Layer Closets, 6 VLANs
- 500 users per VLAN total 3000 users
- 3 VLANs per CAS 1500 users each
CAS Foundation: Centralized Deployment

Example: Collapsed Core Centralized Deployment

- Virtual Gateway Mode
- 6 Access Layer Closets, 6 Data VLANs
- 500 users per VLAN, total 3000 users
- 3 VLANS per CAS, 1500 users each
CAS Foundation: Layer 2 Mode & Layer 3 Mode

- Clean Access Servers have two client access deployment models – Where the client is adjacent?
  - Layer 2 Mode – MAC is unique
  - Layer 3 Mode – IP is unique
- Any CAS can be configured for either method, but a CAS can only be one at a time
- Deployment mode selection is based on whether the client is Layer 2 adjacent to the CAS
CAS Foundation: Layer 2 Mode

- Client is Layer 2 Adjacent to the CAS
- MAC address is used as a unique identifier
- Supports both VGW and Real IP GW
- Supports both In Band and Out of Band
- Most common deployment model for LANs
CAS Foundation: Layer 3 Mode

- Client is NOT Layer 2 Adjacent to the CAS
- IP Address is used as a unique identifier
- Supports both VGW and Real IP GW
- Supports In Band Mode**
- Needed for WAN and VPN deployments
CAS Foundation: In Band & Out of Band

- Clean Access Servers have two traffic flow deployment models
  - In Band
  - Out of Band
- Any CAS can be configured for either method, but a CAS can only be one at a time
- Selection is based on whether the customer wants to remove the CAS from the data path
- CAS is ALWAYS inline during Posture Assessment
CAS Foundation: In Band

- Easiest deployment option
- CAS is Inline (in the data path) before and after posture assessment
- Supports any switch, any hub, any AP
- Role Based Access Control
  Guest, Contractor, Employee
- ACL Filtering and Bandwidth Throttling
CAS Foundation: Out of Band

- Multi-Gig Throughput deployment option
- CAS is Inline for Posture Assessment Only (VLAN swap after posture)
- Supports most common Cisco Switches **
- 3500 XL and up (check release notes)
- Port VLAN Based and Role Based Access Control
- ACL Filtering and Bandwidth Throttling for Posture Assessment Only
Out Of Band Process Flow

1. New MAC Notification sent to CAM (watch for hubs, needs CAM)
2. Unauthenticated client discovery (Agent popup or new traffic)
3. CAS challenges for credentials
4. Client sends credentials to CAS
5. CAS performs Posture Assessment
6. CAM changes VLAN from Auth to Access
## CAS Foundation Summary

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Virtual Gateway mode is usually the easiest integration into existing networks</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Central deployments will make up 99% of designs</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Layer 2 adjacent clients give more options for security with Layer 2 strict mode</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Pay close attention to In-Band math: it’s 1Gig for 1500 users, not 1Gig for the whole network.</td>
</tr>
</tbody>
</table>
Network Design and Deployment: Agenda

1. NAC Appliance Overview
2. Clean Access Server Foundation Concepts
3. **Clean Access Server Deployment Examples:**
   - Layer 2 In Band CAS
   - Layer 2 Out of Band CAS
   - Layer 2 In Band With Wireless Controllers
   - Layer 3 In Band with VPN
   - Layer 3 In Band CAS with Remote Sites
   - Layer 3 Out of Band CAS
4. Clean Access Manager Options
5. Failover Configurations
Network Design and Deployment Tips

- Make the CAS fit the network, don’t make the network fit the CAS!
- License steps can be very useful
- Most customer deployments involve multiple CAS types:
  - Airespace Wireless : L2 IB
  - ASA VPN 3k : L3 IB
  - 6500 LAN Closets : L2 OOB
Network Design and Deployment Tips

- Best practice recommends full redundancy in all cases.
- All components are Active / Standby, sharing a virtual MAC and virtual IP (Serial/Ether Heartbeat).
- Because of the shared MAC L2 connectivity is required between components.
- Redundancy is not shown in the following examples for diagram simplicity only! Every design that follows can, should, and would have redundancy.
Network Design and Deployment Tips

Multilayer Design L2 Dist-to-Dist Link

- VLAN 900
  - L2 Trunk

- Access
  - VLAN 110
  - VLAN 120
  - VLAN 130
  - VLAN 140
  - VLAN 150
  - VLAN 160

- Collapsed Core / Distribution
  - VLAN’s 10, 20, 30
  - VLAN’s 110, 120, 130
  - VLAN’s 140, 150, 160

- VLAN’s 40, 50, 60
- VLAN’s 10, 20, 30
- VLAN’s 110, 120, 130
- VLAN’s 140, 150, 160
- VLAN’s 40, 50, 60
Network Design: Layer 2 In Band

- Client Traffic is always inline, before and after posture assessment
- CAS securely manages traffic:
  - Filters
  - Bandwidth
  - VLAD retag per role
  - User time-outs
- Used for Hubs, Access Points, Unsupported Switches **
Network Design: L2 In Band, Virtual Gateway
Network Design: L2 In Band, Real IP Gateway

- SVI Vlan 10 IPAddress: 10.1.1.1
- SVI Vlan 901 IPAddress: 10.91.1.1
- CAS IP Address: VLAN 10 10.1.1.2
- VLAN 10 10.91.1.2
- CAS IP Address: VLAN 110 10.110.1.1
- CAS DHCP Server VLAN 110 Scope 10.110.1.5 – 10.110.1.100
- Client IP Address 10.110.1.5
- Default Gateway 10.110.1.1
Network Design: Layer 2 Out of Band

- Client is inline before and during posture assessment
- User VLAN is changed and CAS is bypassed only after a successful login
- CAS securely manages traffic only during assessment
- Uses SNMP for traps and switch configuration
- Requires Supported OOB Switches
Network Design: L2 Out of Band, Virtual Gateway
Network Design: L2 Out of Band, VGW with IP Phones

- **DHCP Server**
  - VLAN 10 Scope: 10.1.1.5 – 10.1.1.100

- **CAM IP Address**
  - 10.90.1.2

- **SVI Vlan 900 IP Address**
  - 10.90.1.1

- **SVI Vlan 10 IP Address**
  - 10.1.1.1

- **SVI Vlan 901 IP Address**
  - 10.91.1.1

- **CAS IP Address**
  - 10.91.1.2
  - Management Only

- **.1Q Trunk VLAN**
  - 10, 901

- **.1Q Trunk VLAN**
  - 10.110, 700

- **VLAN 110**

- **VLAN 900**

- **Aux VLAN 700**
  - Access VLAN
  - 10
  - OR
  - 110

- **Client IP Address**
  - 10.1.1.5
  - Default Gateway
  - 10.1.1.1
Network Design: Layer 2 In Band with Airespace

- In Band Required, VLAN assignment is directly related to SSID
- User Traffic VLAN exits the controller, not the AP
- All In Band CAS Security Features still applicable
- Single Sign on Support with 802.1x WLAN Authentication
Network Design: L2 In Band, Airespace
Single Sign On Process Flow

1. AP Challenges 1X supplicant for credentials
2. Controller Forwards credentials to RADIUS
3. RADIUS Forwards credentials to External Database
Single Sign On Process Flow

4. External Database Validates and responds
5. RADIUS Server forwards response to controller
6. User is granted access
7. Controller sends RADIUS Accounting to CAM after login
8. CAM logs user into CCA
9. CAM Forwards RADIUS Accounting to RADIUS
Network Design: Layer 3 In Band

- Client Traffic is always inline, before and after posture assessment
- CAS securely manages traffic:
  - Filters
  - Bandwidth
  - VLAD retag per role
  - User time-outs
- Used when MAC address is no longer unique
Network Design: L3 In Band with VPN concentrator
Network Design: L3 In Band, Virtual Gateway
Network Design: L3 In Band with Multiple Remotes
Network Design: L3 In Band with Remotes & VRF / PBR
Network Design: Layer 3 Out of Band

- Client is inline before and during posture assessment
- User VLAN is changed and CAS is bypassed only after a successful login
- CAS securely manages traffic only during assessment
- Uses SNMP for traps and switch configuration
- Requires Supported OOB Switches
- Requires Agent or Browser Control for MAC **
Network Design: L3 Out of Band
Network Design and Deployment Tips

Routed Access Design L2 Dist-to-Dist Link

Access

Collapsed Core / Distribution

Access
Example: Enterprise Centralized Deployment

Virtual Gateway Mode

- 3 Distribution Layer Building Blocks, 12 Data VLANs
- ~250 (class C) users per VLAN total 3000 users
- 6 VLANs per CAS 1500 users each
Network Design Summary

- CAS selection can become complex, think it through and weigh the pros and cons
- General guideline is to start out with L2 IB VGW
  - Go Real IP Gateway if you want /30
  - Go Out of Band if you want more bandwidth
  - Go L3 if you cannot ensure MAC address
- The simpler the deployment the easier it is to manage going forward!
Q and A
Network Design and Deployment: Agenda

1. NAC Appliance Overview
2. Clean Access Server Foundation Concepts
3. Clean Access Server Deployment Examples
4. Clean Access Manager Options:
   - CAS Configuration
   - Out of Band Switch Profiles
   - Checks, Rules, and Roles
   - Back-end Authentication
   - Logging and Management
5. Failover Configurations
Clean Access Manager: Configuration

- Clean Access Manager uses a GUI front end for administration and management.
- Flat HTML, no Java or Active-X controls are needed.
- Changes are only made once in the active CAM, replication takes care of the rest.
- Communication between the CAS and the CAM is protected by SSL and shared passwords.
- Clean Access Server administration is controlled centrally through the Clean Access Manager.
Clean Access Manager: Configuration

Servers are centrally managed through the CAM

![Cisco Clean Access Manager](image_url)
Clean Access Manager: Configuration

VLAN Mapping for Virtual Gateway Deployments

Device Management > Clean Access Servers > 10.60.10.2

Enable VLAN Mapping

<table>
<thead>
<tr>
<th>Untrusted VLAN ID</th>
<th>Trusted VLAN ID</th>
<th>Description</th>
<th>Del</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>10</td>
<td>Users on edge switch</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>20</td>
<td>Users on edge switch</td>
<td></td>
</tr>
</tbody>
</table>
Clean Access Manager: Configuration

- Multiple DHCP configuration options allow administrators to selectively:
  - Pass-through
  - Relay
  - Respond

- DHCP Server functionality allows additional option bits to be set and passed

- Auto generation tool for subnet management for /30 or other DHCP Server deployments
Clean Access Manager: Configuration

Auto-Generate tool for subnet creation
Clean Access Manager: Out of Band

- Out of Band deployments use SNMP for communication between the CAM and the network devices
- Switches are managed through profiles in the CAM for faster configuration of multiple switches
- Profiles determine on a port-by-port basis which switch ports are managed by Clean Access, default VLAN settings, and Auth to Access logic flows
Clean Access Manager: Out of Band

SNMP controls manage the Out of Band communication
Clean Access Manager: Out of Band

<table>
<thead>
<tr>
<th>Name</th>
<th>Index</th>
<th>Description</th>
<th>Status</th>
<th>Bounce</th>
<th>Initial VLAN</th>
<th>Current VLAN</th>
<th>NAC</th>
<th>Client MAC</th>
<th>Profile</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>1</td>
<td>FastEthernet0/1</td>
<td></td>
<td></td>
<td>TRUNK</td>
<td>TRUNK</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fa0/2</td>
<td>2</td>
<td>FastEthernet0/2</td>
<td></td>
<td></td>
<td>TRUNK</td>
<td>TRUNK</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fa0/3</td>
<td>3</td>
<td>FastEthernet0/3</td>
<td></td>
<td></td>
<td>11</td>
<td>11</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fa0/4</td>
<td>4</td>
<td>FastEthernet0/4</td>
<td></td>
<td></td>
<td>11</td>
<td>11</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fa0/5</td>
<td>5</td>
<td>FastEthernet0/5</td>
<td></td>
<td></td>
<td>11</td>
<td>11</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fa0/6</td>
<td>6</td>
<td>FastEthernet0/6</td>
<td></td>
<td></td>
<td>21</td>
<td>21</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fa0/7</td>
<td>7</td>
<td>FastEthernet0/7</td>
<td></td>
<td></td>
<td>21</td>
<td>21</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fa0/8</td>
<td>8</td>
<td>FastEthernet0/8</td>
<td></td>
<td></td>
<td>21</td>
<td>21</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fa0/9</td>
<td>9</td>
<td>FastEthernet0/9</td>
<td></td>
<td></td>
<td>TRUNK</td>
<td>TRUNK</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fo0/10</td>
<td>10</td>
<td>FastEthernet0/10</td>
<td></td>
<td></td>
<td>TRUNK</td>
<td>TRUNK</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fa0/11</td>
<td>11</td>
<td>FastEthernet0/11</td>
<td></td>
<td></td>
<td>10</td>
<td>31</td>
<td>✗</td>
<td></td>
<td>Control31</td>
<td></td>
</tr>
<tr>
<td>Fa0/12</td>
<td>12</td>
<td>FastEthernet0/12</td>
<td></td>
<td></td>
<td>10</td>
<td>10</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fa0/13</td>
<td>13</td>
<td>FastEthernet0/13</td>
<td></td>
<td></td>
<td>10</td>
<td>10</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fa0/14</td>
<td>14</td>
<td>FastEthernet0/14</td>
<td></td>
<td></td>
<td>20</td>
<td>20</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
<tr>
<td>Fa0/15</td>
<td>15</td>
<td>FastEthernet0/15</td>
<td></td>
<td></td>
<td>20</td>
<td>20</td>
<td>✗</td>
<td></td>
<td>Default [uncontrolled]</td>
<td></td>
</tr>
</tbody>
</table>
Clean Access Manager: Pre-Configured Checks

- Agent updates and pre-configured checks are downloaded automatically from Cisco
- 60 minute connection interval keeps signatures fresh
- Proxy capabilities for customer who do not allow direct internet connections
- SSL encryption and certificates secure traffic between Cisco and the CAM
Clean Access Manager: Pre-Configured Checks

Automatic updates for pre-configured checks

 Cisco Clean Access Manager  Version 3.6.2

Device Management > Clean Access

Certified Devices  General Setup  Network Scanner  Clean Access Agent

Distribution  Rules  Requirements  Role-Requirements  Reports  Updates

Current Version of Cisco Checks & Rules: 10183
Current Version of CCA Agent Upgrade Patch: 3.6.2.0
Current Version of Supported AV/AS Product List: 37
Current Version of Default Host Policies: 5
Current Version of CS Detection Fingerprint: 1

Update Settings
- Automatically check for updates every 1 hours
- Check for CCA Agent upgrade patches
- Use an HTTP proxy server to connect to the update server

Proxy Address: proxy-sjc-1.cisco.com
Proxy Port: 80
Proxy Username:
Proxy Password:

Update  Clean Update
Clean Access posture validation is a hierarchical process with either pre-loaded or custom profiles.

**CHECKS**
- assess the state of a file, application, service, or registry key

**RULES**
- contain single or multiple Checks

**REQUIREMENTS**
- contain single or multiple Rules

**ROLES**
- have one or more Requirements
Clean Access Manager: Checks, Rules, and Roles

CHECKS
Assess the state of a file, application, service, or registry key

- Is anti-spyware installed?
  (application present, file present)
- Is anti-spyware up-to-date?
  (file version > or =)
- Is anti-spyware running?
  (service / exe running)
Clean Access Manager: Checks, Rules, and Roles

Registry Key check for a Windows Hotfix
Clean Access Manager: Checks, Rules, and Roles

RULES
Assemble individual checks together to make a posture assessment

Anti_Spyware_Installed_Check
AND
Anti_Spyware_UptoDate_Check
AND
Anti_Spyware_Running_Check
Clean Access Manager: Checks, Rules, and Roles

Multi-level Check logic with operators
Clean Access Manager: Checks, Rules, and Roles

**REQUIREMENTS**
Tie remediation actions directly to a rule

**ROLES**
Determine which rules apply and what security filters are applied

Remediation methods include:
- File Distribution ("Download antispyware.exe")
- Link Distribution ("windowsupdate.com")
- Local Check (text instructions or messages)
- Definition Update (direct launch of supported AV or AS)

Option to dynamically assign VLANs
Apply individual URL redirection per role, as well as Acceptable Usage Policies, User Pages, and more
Clean Access Manager: Checks, Rules, and Roles

Remediation can be manual, automatic, optional, or enforced
Clean Access Manager: Checks, Rules, and Roles

Roles all have unique requirement lists
Clean Access Manager: Checks, Rules, and Roles

- Role based security determines:
  - What checks and rules apply for posture assessment
  - What security filters are applied
- Dynamic VLAN assignment option for both In Band and Out of Band to additionally segment broadcast domains per role
- Individual URL redirection per role, as well as Acceptable Usage Policies, User Pages, and more
Clean Access Manager: Checks, Rules, and Roles

Per-role fine tuning for timers, agents, and policies

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent

User Role: consultant
Operating System: ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

- [ ] Require use of Clean Access Agent
  Clean Access Agent Download Page Message (or URL):
  <b>Network Security Notice:</b> This network is protected by the Clean Access Agent, a component of the Cisco Clean Access Suite. The Clean Access Agent ensures that your computer meets the requirements for accessing this	
  [ ] Show Network Scanner User Agreement page to web login users
  [ ] Enable pop-up scan vulnerability reports from User Agreement page
  [ ] Require users to be certified at every web login
  [ ] Show Network Policy to Clean Access Agent users
  Network Policy Link:
  [ ] Exempt certified devices from web login requirement

- [ ] Block/Quarantine users with vulnerabilities in role: Quarantine Role (15 minutes)
  Show quarantined users User Agreement Page of: quarantine role

Update  Cancel
Clean Access Manager: Filters and Bandwidth

- Security Filters behave the same as Access Control Lists with additional http://weblink and Layer 2 Protocol capabilities
- Each role has its own filter, with access levels controlled by the system administrators
- Bandwidth controls allow for either per-user or per-role restrictions are very common for remediation and guest access applications
Clean Access Manager: Filters and Bandwidth

Filter display by role at a glance

<table>
<thead>
<tr>
<th>Action</th>
<th>Protocol</th>
<th>Untrusted</th>
<th>Trusted</th>
<th>Enable</th>
<th>Edit</th>
<th>Del</th>
<th>Move</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>TCP</td>
<td><em>:</em></td>
<td>172.19.106.12/255.255.255.0:*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow</td>
<td>ALL TRAFFIC</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow</td>
<td>UDP</td>
<td>DNS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block</td>
<td>ALL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Protocol</th>
<th>Untrusted</th>
<th>Trusted</th>
<th>Enable</th>
<th>Edit</th>
<th>Del</th>
<th>Move</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>TCP</td>
<td><em>:</em></td>
<td>172.19.106.12/255.255.255.0:*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow</td>
<td>ALL TRAFFIC</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow</td>
<td>UDP</td>
<td>DNS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block</td>
<td>ALL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Add Policy to All Roles
Clean Access Manager: Filters and Bandwidth

Bandwidth control per role and per user
Clean Access Manager: Back-end Authentication

- Flexible back-end authentication options allow for fast integration to existing networks
  - Kerberos, NTLM
  - RADIUS
  - LDAP
- Map users attributes and rights directly to NAC Appliance Roles and Filters
- Add operators and conditions to mapping rules to dial in the desired access rights
Clean Access Manager: Back-end Authentication

Multiple back-end authentication options
Clean Access Manager: Back-end Authentication

Mapping rules display the ability to have priority and logic
Clean Access Manager: Logging and Management

- Detailed up to date usage information on Authentications and Posture assessments from:
  - Summary Dashboard
  - Certified Devices List
  - Online Users Pages

- Event logging for all Agent activities, Agent-less Network Scanner, and System Information

- Logs can be viewed locally or sent via Syslog to an off-box collection engine for custom reports
Clean Access Manager: Logging and Management

Administrative control with real time information
Clean Access Manager: Logging and Management

System messages and logs can be viewed right from the console

<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miscellaneouss</td>
<td>Miscellaneous</td>
<td>2006-04-11 01:11:00</td>
<td>Overwrote 2 logs in the past 50 minutes to keep the event log limit.</td>
</tr>
<tr>
<td>Administration</td>
<td>Administration</td>
<td>2006-04-11 00:48:56</td>
<td>Admin user session is created, login succeeded. Name:admin, Group: Full-Control Admin, IP: 10.86.242.55, Login time: 04/11/06 00:48:56, Last access time: 04/11/06 00:48:56</td>
</tr>
<tr>
<td>Miscellaneouss</td>
<td>Miscellaneous</td>
<td>2006-04-11 00:21:00</td>
<td>Overwrote 6 logs in the past 50 minutes to keep the event log limit.</td>
</tr>
<tr>
<td>CleanAccessServer</td>
<td>CleanAccess</td>
<td>2006-04-11 00:21:00</td>
<td>172.18.106.13 System Stats: Load factor 0 (max since reboot: 24) MomFree: 161624 kB, cpu: 2994 125 14271 3235212 952 130 182 0</td>
</tr>
<tr>
<td>CleanAccess</td>
<td>CleanAccess</td>
<td>2006-04-11 00:20:54</td>
<td>Automatic host policy update scheduled at 04/11/06 00:20:02 is successful. Latest version (Ver. 5) of default host policies already installed</td>
</tr>
<tr>
<td>CleanAccess</td>
<td>CleanAccess</td>
<td>2006-04-11 00:20:54</td>
<td>Automatic OS detection update scheduled at 04/11/06 00:20:54 is successful. Latest version (Ver. 1) of OS detection fingerprint already installed</td>
</tr>
<tr>
<td>Administration</td>
<td>Administration</td>
<td>2006-04-11 00:20:52</td>
<td>av_def_date_AhnLabAV, av_def_data_AhnLabAV, av_def_data_AhnLabAV, av_def_data_BrowingAV, av_def_data_RisingAV are modified. All other checks are unchanged</td>
</tr>
<tr>
<td>CleanAccess</td>
<td>CleanAccess</td>
<td>2006-04-11 00:20:52</td>
<td>Automatic rules update scheduled at 04/11/06 00:20:52 is successful. Automatic Cisco Clean Access Agent update scheduled at 04/11/06 00:20:52</td>
</tr>
</tbody>
</table>
Clean Access Manager: Logging and Management

- Administrative User Accounts for change control logging
- Administrators commonly create multiple views for NOC and Help Desk Operations
- Each account has restrictions to each module of the system, permissions are:
  - Full Access
  - Read-Only
  - No Access
Clean Access Manager: Logging and Management

Fine tune Administrative rights and privileges

Administration > Admin Users

- Disable this group
- Group Name: Help-Desk
- Description: Customized permissions for help desk
- Access Control Policy:
  - Clean Access Servers
    - Default Clean Access Server Access: read only
    - Clean Access Server 172.19.166.13: read only
  - Module Features
    - Default Feature Access: read only
    - Clean Access Servers Management: read only
    - Device Filters (MAC & Subnet): full control
    - Roaming: read only
    - Certified & Floating Devices: full control
    - Network Scanner (Nessus): read only
    - Clean Access Agent: read only
    - Switch Management: read only
Clean Access Manager Summary

- Centralized and scalable management and policy configuration
- Pre-configured checks drastically reduce day 2 support and maintenance
- Full access to the rules engine can create a posture assessment for any application
- Flexible remediation options give users as much power as desired to self-repair, reducing help desk dependence
Network Design and Deployment: Agenda

1. NAC Appliance Overview
2. Clean Access Server Foundation Concepts
3. Clean Access Server Deployment Examples
4. Clean Access Manager Options
5. Failover Configurations
Failover Configurations: Manager

In order for the pair to appear to the network and to the Clean Access Server as one entity, you must specify a Service IP address to be used as the trusted interface (eth0) address for the cluster.

To create the crossover network on which high-availability information is exchanged, you connect the eth1 ports of both Managers.

The Manager then creates a private, secure two-node network for the eth1 ports of each server to exchange UDP heartbeat traffic and synchronize databases.

License key only to primary Manager. It will be copied over automatically.
### Failover Configurations: Manager

**Administration > Clean Access Manager**

<table>
<thead>
<tr>
<th>Network &amp; Failover</th>
<th>System Time</th>
<th>SSL Certificate</th>
<th>System Upgrade</th>
<th>Licensing</th>
</tr>
</thead>
</table>

#### Network Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>172.16.1.42</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>172.16.1.40</td>
</tr>
<tr>
<td>Host Name</td>
<td>cam4</td>
</tr>
<tr>
<td>Host Domain</td>
<td></td>
</tr>
<tr>
<td>DNS Servers</td>
<td>4.2.2.4</td>
</tr>
</tbody>
</table>

#### Failover Settings

- **High-Availability Mode**: HA-Primary

  (for high availability, set up the primary server before the standby)

- **Service IP Address**: 172.16.1.41

- **Peer Host Name**: cam4sec

- **Heartbeat UDP Interface**: eth1

  (HA on eth1 interface is enabled by default. A serial port can additionally be configured.)

- **Heartbeat Serial Interface**: N/A

#### Crossover Network Interface Setting

- **Crossover Network**: 192.168.0.1252

- **Crossover Netmask**: 255.255.255.252

[Update]  [Reboot]
Failover Configurations: Server

- The standby monitors the health of the primary server via a heartbeat signal exchanged on a dedicated Ethernet and/or serial connection.

- A Service IP address is the common IP address that the external network uses to address the pair.

- If the Clean Access Servers will operate as DHCP Servers (not in DHCP relay or passthrough mode) additional configuration steps needed.

  DHCP information, such as information regarding active leases and lease times, is exchanged by SSH tunnel.
Failover Configurations: Server

<table>
<thead>
<tr>
<th>Administration</th>
<th>Network Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>DNS</td>
</tr>
<tr>
<td>Failover</td>
<td>DHCP Failover</td>
</tr>
</tbody>
</table>

**Current Status**
- **Local Node**: OK [Active]
- **Peer Node**: OK

- **Clean Access Server Mode**: HA-Primary Mode
- **Trusted-side Service IP Address**: 10.40.3.2
- **Untrusted-side Service IP Address**: 10.40.31.1
- **[Primary] Local Host Name**: cas4
- **[Primary] Local Serial No.**: 00.12.79.93.10.2E.00.12.79.93.10.4F
- **[Primary] Local MAC Address**: 00:12:79:93:10:4F
- **[Standby] Peer Host Name**: cas4sec
- **[Standby] Peer IP Address**: 10.40.3.4
- **[Standby] Peer MAC Address**: 00:01:02:03:04:05
- **Heartbeat UDP Interface**: eth0
- **Heartbeat Serial Interface**: N/A
- **Heartbeat Timeout (seconds)**: 10
  - (make longer than 10 seconds)
- **Enable Serial Login**: Enable
  - (Serial Login disabled by default when HA mode selected)

[Update Reboot]