



Cisco Security Deployment Methodologies - NAC



Michael Jones

michjone@cisco.com

Security Services Specialist

Network Security Policy Continuum

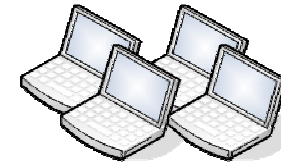


1. Network Security Policy

3. Identity Mgmt

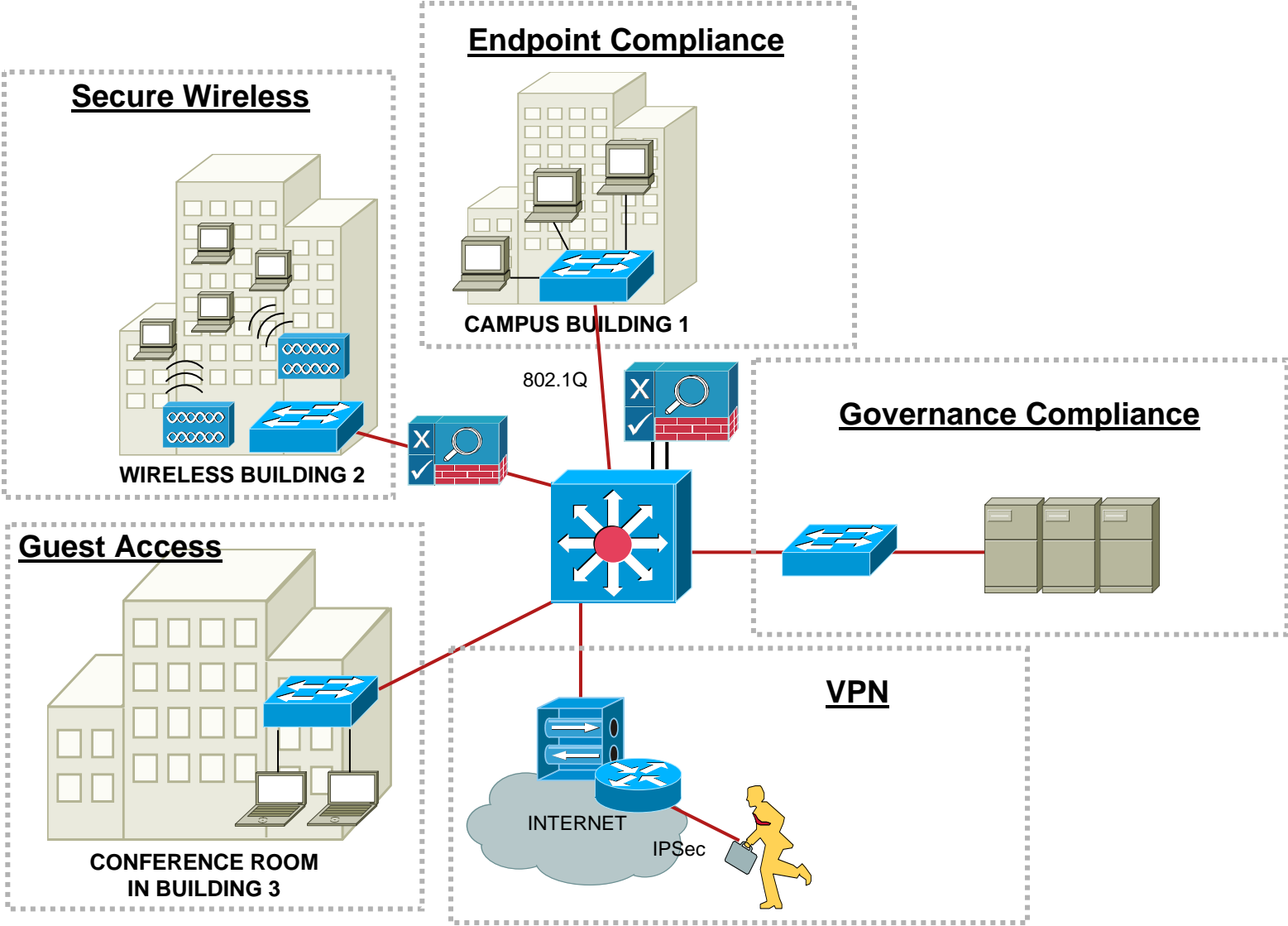


2. End Point Compliance



NAC = All 3 Working Together

Cisco NAC Covers Broad Use Cases



Agenda

Scoping and Approach Overview
Identifying Client Contacts
General Requirements Gathering
Technical Requirements Gathering
Design Phase
Test Plan
Tips From The Field

Scoping and Approach Overview

- Information that will help in scoping:
 - AD Single Sign On
 - Number of Switches
 - Number of People
 - Number of Sites
 - Deployment Type
 - Profiler
 - Guest Access
 - Differentiated Policy Enforcement
- A phased approach will ensure success
 - Requirements Gathering and Environment Analysis
 - Design Session
 - Lab Configuration and Testing
 - Pilot Implementation
 - Knowledge Transfer
 - Enterprise Deployment Planning

Assignment of Roles and Responsibilities

- **Project manager** – responsible for ensuring deliverables are met in time and within budget. This individual has day-to-day responsibility for managing the implementation team and is the first point of escalation for the client.
- **Technical lead** – engineer responsible for the design and implementation of the NAC Appliance solution. This individual must have extensive experience with NAC Appliance deployments.
- **Implementation engineer** – Depending on the size and scope of the project, additional Cisco engineers will participate in the NAC Appliance implementation. These engineers must have basic NAC Appliance training and experience with NAC Appliance implementations.
- **Engagement manager** – individual that has overall responsibility for the quality of the deliverable. This role is typically played by the Cisco Advanced Services manager. In some accounts, the Cisco account manager might play this role.

Identify Client Contacts

- **Main project contact** – this is the single point of contact for assisting the project manager with the coordination of all project activities. Because of their internal knowledge of the organization, it is preferred to have a single client contact help coordinate all internal activities. This individual will work closely with the Cisco project manager to ensure progress is made according to schedule and budget. This individual is responsible for identifying client contacts for addressing the roles discussed in the following sections
- **Information security contact**– identify the individual responsible for setting the corporate information security policy. It is recommended that this individual:
 - Approves the security requirements
 - Sets policy for which NAC Appliance requirement will be enforced
 - Provides direction with respect to the remediation process
 - Understands the current security policies for each IT domains (LAN, WAN, wireless, remote access, extranet, desktop, server, applications)
 - Knows the policy on unmanaged or non-standard machines on the network
 - Understands how access to the network handled
- **System administration contact**– identify a system administration contact to support the project. The responsibilities of the system administrator will be to:
 - Provide documentation about the Proxy servers
 - Provide documentation about the servers if external remediation servers are used
 - Provide documentation about the DHCP servers - we should also talk about AD configuration as well

Identify Client Contacts - Continued

- **Network Administration contact**– identify a network administration contact to support the project. The responsibilities of the network administrator will be to:
 - Configure the NAC Appliance server (IP address, DNS, NTP, Physical connection to the network, etc.)
 - Provide list of IP subnets to be managed by NAC Appliance
 - Certify NAC Appliance implementation does not have a negative effect on network performance
- **Network Management contact**– identify a network management contact to support the project. The responsibilities of the network management contact will be to:
 - Provide the network management host (syslog and SNMP trap sink information to monitor overall health of NAC Appliance devices)
- **Desktop Support Engineer(s)**– identify a desktop support engineer contact to support the project. The responsibilities of the desktop security engineer contact will be to:
 - Provide a list of applications/services (such as CSA, Anti-Virus, Anti-Spyware, SUS client, etc.) to be added in the NAC Appliance for posture assessment - this was under the information security contact as they would be the ones dictating the policy - does this mean that this group will give us the versions etc?
 - Provide information about how the application is installed and works
 - Provide exempt device information, such as printers and fax machines
 - Provide exception to the desktop firewall rule to allow NAC Appliance Agent discovery process
- **Software deployment Engineer(s)**– identify a software deployment engineer contact to support the project. The responsibilities of the software deployment engineer contact will be to:
 - Provide ways to deploy NAC Appliance agent to the desktop
 - Provide information on how desktop application (such as CSA, Anti-Virus, Anti-Spyware, SUS client, etc.) are deployed

Identify Client Contacts - Continued

- **VPN concentrator administrator(s)**– identify a VPN security contact to support the project. The responsibilities of the VPN security contact will be to:
 - Provide a list of VPN devices (such as VPN3000 and ASA) to be added in the NAC Appliance as a floating device and SSO
 - Provide RADIUS accounting information for the VPN devices
- **Network Access Services administrator(s)**– identify a network access services contact to support the project. The responsibilities of the contact will be to:
 - Provide a list of AAA Servers (such as ACS that should to be added in the NAC Appliance for Authentication and Accounting)
 - Provide logging information about the AAA servers
- **PKI Certificate Server Administrator(s)** – identify the PKI CA server contact to support the project. The responsibilities of the CA server contact will be to:
 - Provide information on current PKI solution
 - Provide/understand migration, support, and scaling issues of self-signed certificate
 - Provide/generate server certificate for NAC Appliance Manager and Server
 - Assist the project manager with deploying root certificate if necessary
- **Operations contact** – identify an operations contact that will represent the organization responsible for day-to-day management of the NAC Appliance (once implemented). The responsibilities for the operations contact will be to:
 - Provide operational requirements
 - Support NAC Appliance deployment efforts by monitoring impact to operations
 - Accept the NAC Appliance implementation (i.e. certify overall requirements are met)

Identify Client Contacts - Continued

- **Quality assurance contact(s)** – identify testing contact(s) for the suite of protected applications. The responsibilities of the QA individuals will be to:
 - Support the NAC Appliance requirement and remediation tuning processes by performing complete integration of all the supported applications on the desktop
 - Certify NAC Appliance implementation has no negative impact on the network
- **Customized application subject matter expert(s)** – identify individuals that understand how some of the non-supported devices or home-grown applications work. They have a detailed understanding of the application's internals. The responsibility of the subject matter experts is to assist in the creation of custom checks/rules.
- **NAC Appliance engineering contact(s)**- identify the client contacts that will be responsible for future NAC Appliance engineering efforts. The responsibilities of these individuals will be to:
 - Pursue formal NAC Appliance software training to ensure they can support future NAC Appliance deployments.
 - Gain a detailed understanding of the NAC Appliance software installation and configuration process
 - Shadow the Cisco engineering team to learn the NAC Appliance implementation methodology
- **Help Desk** -Provide information on how support calls are handled/triaged -Provide information on end-user communications
- ***Kick-off meeting***
 - State the business objectives for the project
 - Introduce the NAC Appliance implementation team
 - Review Major NAC Appliance implementation tasks, such as project dates and major milestones
 - Schedule meetings with key players to start the requirements analysis phase

General Requirement Analysis

- Security Policy Creation and Maintenance

Are the network (LAN, WAN, wireless, remote access, extranet) and IT (desktop, server, applications) teams cross-functional or dys-functional? How often do they meet and discuss security updates and policy changes?

What are the current security policies for each of these respective domains?

Who (or what group) is responsible for policy creation? Policy enforcement?

What is the quorum for making changes?

Will network access authorizations be based on identity, posture, or both?

What is the policy on unmanaged or non-standard machines on the network (labs, guests, consultants, extranets, kiosks, etc.)?

How will acquisitions that may have a different network infrastructure and policy be handled?

- Public Key Infrastructure (PKI)

Has an enterprise PKI solution been deployed? Windows 200x Server, CA vendor, or other?

If not, will one be installed and managed, or will individual certificates be purchased from a CA vendor?

Are the long-term support, migration, and scaling issues of self-signed certs understood?

- Directory Services

Have directory services been deployed: Microsoft Active Directory, LDAP, or other?

Will Single Sign on be a requirement?

General Requirement Analysis - Continued

- Network Access Devices (NADs)
 - What type of switches will the NAC Appliance interact with?
 - Switch model
 - IOS/CatOS code level
 - Do the NADs have enough memory for the larger IOS security images? Memory upgrade?
- Hosts and Other Network Attached Devices
 - Are there enough licenses for all of the software that will be required on each device?
 - Will licenses be provided for the mandated software to employee home computers, guests, extranet partners, etc.?
- NAC Agentless Hosts (NAHs)
 - Have the various NAH device types in the network been identified:
 - No CAA (unsupported OS, network boots)
 - Otherwise unmanaged/uncontrolled devices (guests, labs, etc)
 - What is the authorization strategy for NAHs?
 - Whitelisting by port, mac-address, ip-address, wildcard, profiler?
 - Is guest access a requirement? If so how will that be handled?
 - Is there a personal firewall on end-hosts that would block Discovery Packets/NAC Appliance ports? (UDP: 8905,8906, TCP: 8910,443,80)

General Requirement Analysis - Continued

- Patch Management

 - What update/patch/remediation software is currently in use, if any?

 - Does this update software integrate with NAC?

 - Will there be a remediation web site for communicating posture status to unhealthy and/or nonresponsive users?

 - Will software be distributed to employees and/or guests from this site? How will the licensing be handled?

- Monitoring, Reporting, Troubleshooting

 - What is the existing monitoring and reporting framework?

 - Will NAC logs and events integrate into the current logging environment? Or is something additional needed?

 - What is the long term storage for all of these new logs and events?

- Communications

 - How are the following achieved: Awareness (need, benefit), Readiness (what, when), Adoption (monitoring, enforcement)

 - Email, internal news, remediation web site, support desk?

- Support Desk

 - Staff will require training for new technology and process.

 - How will the support staff troubleshoot support calls related to NAC?

 - What application development is required to resolve NAC-related issues?

Technical Requirement Analysis

- Integration of network - Required information includes device vendor, OS version, IP addresses, device name
 - VPN and/or wireless controllers (including RADIUS server and IP/MAC address)
 - Layer 2 switches (including SNMP RO and RW strings, VLAN information)
- Integration of desktop applications - Required information includes supported OS, AV/AS vendor, AV/AS version, service/application name, file entry, registry entry to check for
 - Cisco CSA
 - Anti-Virus/Anti-Spyware
 - SUS
- Integration of authentication - Required information includes server IP, service port, and service account name and password, etc.
 - RADIUS
 - AD
 - LDAP
- Integration of remediation server - Required information includes server IP, host name, service port
 - SUS server
 - Web server hosting installation files
 - ePO, LiveUpdate server

Technical Requirement Analysis - Continued

- Integration application deployment tool such as:
 - CA SDO
 - Altiris
 - Marimba
- Integration of OS - Required information includes OS version and patch levels
 - Windows
 - MacOS
 - Linux
- Document list of trusted DNS servers - Required information include DNS server IP addresses
- Document list of web proxy servers - Required information include proxy server IP addresses and port numbers and also auto proxy script server if present
- Integration of network management servers - Required information includes IP addresses and community
 - Syslog server
 - SNMP trap sink

Technical Requirement Analysis - Continued

Network Infrastructure Information

- Detailed information on the sites that the solution will be piloted at including:
 - Access layer switch info (code level/hardware type/ip address/visio) for all switches
 - Visio Diagram of the LAN layout
 - How many people are at the site
 - Is VOIP being used?
 - Is VTP being used - if so what mode is it running in
 - Is there wireless access - is the wireless access a network of convenience or considered production always needs to be up
 - How is the wireless network designed
 - What does the wan connectivity for these sites look like
- For the remainder of the network is it possible to generalize the rest of the sites into categories
 - example: manufacturing plants - 6500's in the core, 3500 at access layer, x amount of people, 2 3745 routers for wan connectivity back to corp -- administrative centers - 6500 in core, 2900 access layer etc
- Global Wan layout - Visio Diagram
- Where do vpn's terminate?
- How is internet access handled? (one pop? multiple pops? proxy?)
- Are applications served out of the data center with file and print access servers located at the sites?

Operational Requirement Analysis

- NAC Appliance backup/restore requirements
- NAC Appliance redundancy requirement
- Network connectivity (i.e. required open TCP/UDP ports) requirements for the NAC Appliance Manager to manage NAS
- NAC Appliance training required for operations personnel
- Documentation required for operations acceptance
- Technical support requirements and escalation process
- NAC Appliance maintenance procedures
- System health alerts and notification requirements


Design Phase

- Select a place to add the NAC Appliance in the existing network infrastructure.
- Determine the number and location of the NAC Appliance (Server and Managers) that need to be deployed. The number of required NAC Appliance depends on the following factors:
 - Number of users managed
 - Number of sites managed
 - Number of NAS deployed
- Determine the following:
 - Inband or Out of Band
 - Real Ip or Virtual Gateway
 - Central or Edge
- Determine if a Super Manager is needed for a centralized monitoring architecture
- Meet with information security and network administration to discuss network security requirements for the NAC Appliance server. Since the NAC Appliance runs a strip down version of Linux, most of the services are already disabled. The required network services are already enabled on the NAC Appliance
- Create a high level and low level design for lab and pilot
- Start off with authentication only to ensure that the NAC Appliance is forcing agent pop-ups
- For solutions that require customized checks/rules, these policies must be developed in conjunction with the implementation of the pre-defined policies.
- Create a table that maps all requirements into NAC Appliance software functionality. Where gaps are identified, client's expectations have to be managed to ensure no surprises on the delivered solution.

Building a Test Plan

- Assist in developing a test plan
- Review test plan with all identified client contacts
- Assist in developing success criteria
- Test Plan should include things such as:
 - High Availability - CAS/CAM
 - Pre-Configured Rules update configuration
 - Agentless Web configuration
 - Impact of NAC Appliance Agent on client critical applications
 - NAC Appliance Manager logging and reporting configuration
 - SSO
 - Roles and Filters

Building a Test Plan - Continued

 Test Case Details	
Title	Loss and Restoration of a NAC Appliance Server
Description	Observe and document impact of the following on network access (results recorded from user experience, network event log and management interface)
Priority	High
Automated	No
Operating System	WXP-PRO
Test Setup	<ol style="list-style-type: none"> 1. Users already logged in and CAS fails 2. CAS fails and users try to login
Procedure	<ol style="list-style-type: none"> 1. Standard user logs into VPN 2. Shut down primary CAS 3. After failover re-enable primary CAS eth2 4. Currently logged in user continue to pass traffic 5. Log a second standard user into VPN 6. Shut down secondary CAS eth2 on switch 7. Log in a third standard user into VPN 8. After failover re-enable secondary CAS eth2
Scenario	Wired
Pass/Fail Criteria	<ol style="list-style-type: none"> 1. CAS must failover both ways 2. Users that were currently logged into VPN should not have been kicked out/repostured and able to continue work after failover 3. New user logging into VPN should be postured and then allowed access

Lab Construction

- Assist customer in setting up a lab environment
- Conduct lab configuration according to Lab LLD
- The lab should be a good representation of the production environment
 - Different types of desktop images
 - Different types of hardware
- Assist in lab testing
- Re-verify Pilot or Enterprise LLD based on the results of the test plan
- Have Go/No-Go session to review results, success criteria and pilot/enterprise deployment strategies

Pilot Implementation

- Cutover Meeting to review success exit criteria
- Stage necessary components according to Pilot or Enterprise LLD
- Cutover components according to cutover strategy
- Execute cutover test plan
- Go/No-Go for continued phased deployment

Knowledge Transfer

- Provide on-site knowledge transfer
- Provide ad-hoc sessions during design, lab and implementation
- Conduct formal training sessions

