THE UNIVERSITY of NEW MEXICO

Project Request & Project Plan

Network Access Control

Plan Version:	2.1
Last Updated:	Dec. 1 , 2008
Date Submitted:	Nov. 26, 2008
Submitted by:	Paul Chang
Executive Sponsor:	Paula Loendorf
Expected Start Date:	TBD
Expected End Date:	TBD

Definitions needed: Suggestions highlighted in yellow

Part 1: Project Request

1. **Project Summary (***What will this project accomplish?*)

   Network Access Control (NAC) is an approach for enforcing our organization's security policies on all devices seeking network access. Network Access Control (NAC) allows only compliant and trusted endpoint devices, such as PCs, Laptops, and PDAs, onto the network, restricting the access of noncompliant devices, and thereby limiting the potential damage from emerging security threats and risks. NAC will provide a powerful, roles-based method of preventing unauthorized access and improving network resiliency.

2. **Problem / Need Statement (***Why is this project being proposed?*)

   Information Technology Services has implemented intrusion prevention systems at the network perimeter to prevent potential threats from outside intrusions. While this remains a valid and essential approach, we realize that a large number of threats may also originate from within our network. It is increasingly likely that endpoint devices will introduce virus, worms or malicious threats that are capable of causing significant harm to business critical networks and systems, especially those originating from unknown sources such as guest devices.

   Protecting the network from these threats is an overwhelming challenge. NAC provides automated enforcement and remediation of end point security and is essential in minimizing threats and ensuring policy compliance for network access.

3. **Overview of Project Scope and Objective(s) (***What are the goals of this project, and what is in scope?*)

   The purpose of this project is to implement Network Access Control (NAC) on the campus network infrastructure. The overall goal of NAC is to prevent compromise of the hosts that connect to a network or other network resources and thus the network itself. NAC will be designed for scalability utilizing a vendor neutral solution. NAC will serve the main, north (HSC/UNMH), south and branch campuses as well as the remote access vectors such as VPN services. NAC will eventually extend to State IDEAL identity management.

   The scope of this project is to identify the milestones necessary to successfully and tactfully deploy NAC in a phased approach.

   Implementation Phase I: Authentication only (using LDAP the main UNM Password Database)

   a) Proof of concept – ITS (South & North locations)
   b) Staged wireless deployment for rest of the campus – LoboWiFi and Lobo Sec
   c) Staged public wired deployment on campus

   Implementation Phase II: Deployment security controls

   a) OS and Application patch level enforcement; AV / Malware enforcement, etc.
   b) Role and rule-based access controls

   Implementation Phase III: deployment to partners and rest of main campus

   a) Branch campus locations
   b) HSC / UNMH

c) Full wired deployment
The phases noted above need not be entirely linear.

4. **Summary of Approach (***How will the project objectives be realized?*)
   NAC should be deployed in phases. NAC may be deemed a strategic enterprise initiative but the Network Access Control project should still follow a classic, "crawl, walk, run" model. NAC deployment should start as a learning and fact finding process and gradually become more hardened, secure, and automated over time. Staging the NAC implementation over formal project phases will lead us to progressively improving the benefits of NAC and the best overall results.

5. **Project Benefits / Impact** *(Include quantitative as well as qualitative benefits*)
   Some of the benefits for NAC are:
   - safeguard the network from potential threats
   - control guest machine or non standard device access to network resources
   - consistent access across remote access, wired and wireless networks
   - process for NAC policy enforcement for endpoints
   - role-based network authorization
   - may be used for wireless rogue access point policy enforcement
   - may be used for broadcasting messages for planned network outages or emergencies
   - compliance with patch management, security, asset management, and antivirus standards
   - may be used for P2P file sharing policy enforcement

   IMPACT:
   To understand NAC's impact on our network, we need to understand the degree to which it mandates changes, if any, to our endpoints, switches, VLANs or ACLs, and identity stores. The more we can reduce this impact, while still gaining significant control over what users can do on the LAN, the greater the return on investment from a "time to deploy" perspective.

   Strong dependency on establishing campus wide network use policy to move from phase I (authentication) only to phase II (security control)It will be essential to identify a solution that is scalable, allows for a phased implementation approach while minimizing the impact on technical staff and resources and as transparent as possible to end users.

1. **Alignment with Strategic Priorities**
   The CIO requests that Information Technology Services provides a reliable and resilient network for University Faculty, Staff and Students to utilize in accessing the necessary data to accomplish the University's mission. Network Access Control is a core strategy to achieve this..

2. **What are the consequences if this project is not completed?**

   In this globally dynamic and diverse world, it's impossible to determine where a user's managed or unmanaged device has been before it attempts to access the enterprise network. A user's device could be infected with insidious, virulent forms of malware spawned by today's sophisticated, well-funded hacker. A user's device could be acting as a transfer agent for the spread of viruses, spyware, adware, Trojans, worms, bots, rootkits, or other malicious applications, onto the enterprise network or directly to other unsuspecting user devices. The introduction of any of these unwanted infections can put an organization's intellectual property at risk and it can have a serious impact on productivity, significantly increasing costs to the enterprise.

3. Project Roles & Responsibilities

Project Role	Project Responsibility	Name	Dept & Title	Estimated Time Commitment
Executive Sponsor	An executive-level manager who interacts with the project team leader and acts as liaison with other executive staff members in taking high-level responsibility to champion, guide, and monitor a given project.	Paula Loendorf	Director ITS	
ITS Management Sponsor	Provides technical authority and guidance and maintains the ITS project priorities	Gary Bauerschmidt		
Project Manager	Defines and maintains project plan. Responsible for all project activities.	Paul Chang		
Customer Management Sponsors	Solicit input from user groups that represent customers impacted. Such as Mike Campbell and Rick Adcock	Ivan Boyd Rick Adcock Mike Campbell		
Technical Lead	Leads development and assures knowledge baseis created as well ascommunications requirements anddocuments. Defines, plans, controls, and leads the work of the technical participants. Coordinates integration with existing systems.	Paul Chang		
Project BPOs / Steering Committee	Key Business Process Owners participating in and/or affected by project	Mark Reynolds Michael Carr Gary Bauerschmidt Dave McGuire Jane McGuire		
Project Team (meets weekly)	Project facilitating/appliance hosting/report/stats	Paul Chang	Network Engineer	6 hr/Week pending product selection
	Security Policy requirements	Jeff Gassaway	IT Security Analyst	3 hr/week
	Incident management and user education	Tracy Hart	Technical Project Manage	3 hr/week
	DHCP and DNS service interface	Stephen Smoogen	System Analysis	2 hr/week
	Subnet allocation deployment/troubleshooting	John Duran	Network Engineer	3.5 hr/week
	HSC/UNMH requirements and deployment strategy	Barney Metzner	IT System Manager	1.5 hr/week
	HSC/UNMH requirements and deployment strategy	John Root	Security administrator	1.5 hr/week
IT Security	Security approvals. Use policy and posture assessment requirements	Jeff Gassaway	IT Security Analyst	
Other Stakeholders (meets monthly)	Other stakeholders who should be consulted. Virus check software compliance.	ASUNM (Ivan Boyd) IT UNM IT Agents		

4. Project Request Approvals *(Those providing approval for Part 1, the Project Request)*

Date Reviewed:

Comments:

Reviewers:

Name	Dept & Title	Signature

Part 2: Project Plan

5. Major Project Milestones and Deliverables

(Milestones are significant events; deliverables are outcomes or products that are produced as part of the project)

Deliverable / Milestone	Phase	Mile-stone?	Planned Completion Date	Owner	Resources Needed
1. Begin project - Develop Project Scope of work ; vendor evaluation and get approved by IT leadership	1	Y			
2. Vendor selection and procurement	**1**		**Committee recommended vendor product can be purchased via WSCA contract; otherwise RFP process take 6 to 12 weeks turnaround time**		
3. Establish roll out timeline and milestones	**1**				
4. Implement NAC using established policy enforcement rules.	**2**	**Y**			
5. Train support center and administrative staff on the technology and ensure all fastinfo documentation reflects the NAC solution.	**1**				
6. Implement and test at ITS buildings (wired and wireless)	**1**				
7. Roll out to pre-approved locations	**1,2,3**				
8. Roll out to POD locations	**1**				
9. Roll out to the remainder of campus wireless and wired networks	**1, 3**				
10. Roll out to Remote Access vectors (VPN and Dialups)	**3**				
11. Roll out to North Campus including HSC/UNMH	**3**				
12. Roll out to South Campus	**3**				
13. Roll out to Branch campuses and WAN sites	**3**				

6. Scope *(In order to help define the limits, expectations, and dependencies of this project, list any business functions, systems, projects, groups, and technologies that are supported, impacted, or dependent upon this project as well as those that are not, and those that are uncertain.)*

Scope Element	In Scope / Out of Scope / Uncertain
1. ITS Scope Team – Identify and evaluate the NAC solution	
2. ITS Information Assurance – Provide feedback on NAC solutions and create NAC and Antivirus Policies, develop security requirements for NAC	
3. ITS Systems Group – DNS integration	
4. ITS Communications Group – Campus PR and communications plan	
5. ITS Support Center – FastInfo documentation creation and system training for client facing issues. 6. ITS –Need to have method to distribute anti-virus software quickly and efficiently to mass of users	

7. Assumptions, Constraints, and External Dependencies/Interdependencies (*This plan is based on the following assumptions, constraints, and dependencies/interdepencies.)*

Assumption / Constraint / Dependency
1. Michael Carr - Information Assurance – Phase I authentication and authorization; Policy creations for NAC and Anti Virus standards, develop security requirements for Phase II
2. Jane McGuire - Public announcements and overall campus communication (communications plan)
3. ITS Scope group evaluate/identify NAC solution
4. ITS—Method to distribute anti-virus software quickly and efficiently to mass of users
5.

13.Communication Plan *(How will stakeholders be kept involved and informed about the project status?)*

Audience/Stakeholder	Method of Communications	Frequency

14.Risk Mitigation Plan *(Use H, M, or L for Likelihood and Impact estimates)*

Risk Factor	Likeli - hood	Impact	Risk Plan or Mitigation Strategy	Person Responsible	In Place By
1.					
2.					
3.					
4.					
5.					

15. Project Budget *(Give title of each person working on project. Budget should include **line item detail** for each category)*

	Area			Functional Dept. Project Costs	ITS Project Costs	Functional Dept. Recurring Costs	ITS Recurring Costs
UNM Internal Dollars/Non-Discretionary	**STAFF HOURS**	**Hrs**					
	Student 1. Person 1 Title 2. Person 2 Title	TBD					
	Financial Aid						
	Finance						
	HR/Payroll						
	Shared Components						
	Budget						
	Advancement						
	Platforms/Systems	TBD					
	Database						
	Network/Telecom	TBD					
	Customer Support	TBD					
	Total - Internal Labor ::::::::::						
Discretionary Funds	**Hardware** *(Description & Vendor Name)*	**#Units**	**$**	TBD			
	1.						
	Software *(Description & Vendor Name)*	**#Units**	**$**	TBD			
	1.						
	Staff Training *(Description & Vendor Name)* *Keep in mind fixed costs while in training…*	**Hrs**	**Rate**	TBD			
	1.						
	Consulting /Term *(Include Travel & Other Expenses)* *Keep in mind standard rates, e.g. SIG, SCT, etc…*	**Hrs**	**Rate**	**TBD**			
	1.						
	Other Costs			25% contingency			

			For proof of concept project: $130 K per 10,000 users With 20% on-going maintenance Campus wide deployment of 30,000 concurrent users : $350 K with 20% on-going maintenance			pending scope
Total - External Costs ::::						
GRAND TOTAL :::						

16.Capital Funding Sources (*Note procurement approaches)*

Year end surpluses and other sources that the CIO identifies

Index Code	Budget owner	Amount	Limitations (if any)

17.Recurring Funding sources

If Identified:

Index Code	Budget owner	Amount	Limitations (if any)

If Not Identified:

Person responsible for budget request:

Funding options:

1.
2.

18. Project Plan Approvals

Date Reviewed:

Comments:

Reviewers: *(Those providing approval for Part 2, the Project Plan)*

Name	Dept & Title	Signature