Global Information Assurance Certification Paper

Name: Donald Murphy
Version: 1.4b

Extranet Access Management

Introduction

The following document is an analysis of the business needs and technical solutions for Extranet Access Management (EAM). The document then offers a very high-level implementation plan. The terminology related to this security domain is inherently confusing. The terms Identity management, Single Sign On, Intranet Content Security, Provisioning as well as Extranet Content Management and others are commonly used and have substantial overlap in implementation and function. Adding to the confusion are vendor interpretations of these concepts, their own 'proprietary' nomenclature and a myriad of technical architectures to achieve similar functionality. Although this analysis and project plan incorporates Single Sign On and Provisioning in the latter phases, we will continue to use the term Extranet Content Management as the general topic. Broadly defined, Extranet Access Management is the capability to restrict access by user or group to specific web page or URL. As part of that capability, is the ability to create rules and policies that use existing data stores or directory services.

To sanitize the document, the organization for whom the analysis was performed and the employer of the writer will be referred to as *THE BANK*. The company which has been recently acquired will be referred to as *COMPANY X*. This analysis takes into consideration the existing environment of *THE BANK* and is weighted to solutions that can be implemented in that environment. The document follows a fairly simple business case format, which is complimented with some vendor comparisons of available solutions. The vast majority of the research was completed through the Internet, including the vendor's web sites. This project and analysis are not fictitious and have already been presented to Senior IT Management at *THE BANK.* The project will soon be presented to the Executive Council of *THE BANK* for formal approval.

Analysis and Business Case for Extranet Access Management

Statement of Need

There is a demonstrated and immediate need for Enterprise level Extranet Access Management. There have been an increasing number of business requests to publish and secure documents and manuals on the Intranet. Currently there is no efficient or centrally managed method to accomplish this. Additionally, an 'Intranet Content' Standard has been created. This standard states that any content not intended for public distribution must have access secured to appropriate parties. Thus, a scalable mechanism for securing Intranet content needs to be established at *THE BANK*.

Current Environment

The vast majority of *THE BANK's* Intranet is unsecured. This ranges from departments publishing sensitive information on departmental NT servers to 'content-managed' documents being hosted on Enterprise Intranet servers. All content and applications that have been secured today has been done through FileNet's limited security capabilities or as 'one-off' programming efforts.

There are two centrally supported methods of securing content on the Intranet today.

1) Use of FileNet Document Services and a FileNet administrative application.

2) Use of FileNet Document Services in conjunction with a Cold Fusion 'front-end' to accept a login and authenticate to NDS.

Table 1 highlights the strength and weakness of existing methods.

Table 1, Strengths and weaknesses of existing methods

Method	**Strengths**	**Weaknesses**
FileNet Document Services Security	Provides document level access control	No interface with NDS or ACF2.
	No development required.	Separate FileNet password
		No password expiration or formation rules.
		Separate Administration
Method	**Strengths**	**Weaknesses**
Cold Fusion Front End	Authentication to NDS tree	No ability to delegate administration to business lines
		No granular levels or role-based security
		Cannot be indexed into Intranet searches
		Security model requires NCS and developer effort.
		Lacks scalability,

Scope

The scope of this project is broken into 4 phases. Phase 1 is to secure existing Intranet content as required by the business needs as well as a means to secure additional content as the requirements are delivered. Additionally within the scope of phase 1 is to establish the ability to both centrally manage roles and to delegate management of specific content areas to business units as appropriate.

Phase 2 of this project focuses upon using the same securing mechanism to secure Intranet-facing applications, relieving the Web Development team from having to code this security and providing a consistent and auditable security model.

Phase 3 of this project focuses establishing a 'Single Sign On' capability for specific groups of internal and external customers, again utilizing the tools used in the first two phases.

The scope of Phase 4 of the project will be to establish 'User Rights Provisioning' for all core bank systems (i.e. LAN access, mainframe, email, time reporting, etc.). This will likely require additional software and hardware.

Proposed Environment

THE BANK needs to improve its current technology by deploying a solution that can:

1) Leverage existing user entitlement stores (NDS, ACF2, Active Directory).
2) Provide centralized management and monitoring of Extranet Access.
3) Provide delegated management of specific content areas to business lines as appropriate.

Available Solutions

In-house Developed Solution

There are several reasons that would make in-house development an undesirable choice.

i. The in-house technology currently available (Cold Fusion, etc.) will not scale easily and will require an iterative process for establishing and maintaining security on Intranet.
ii. The time and resources required for developing a comprehensive in-house solution would likely exceed the cost of purchasing a vendor package.
iii. There is currently a converging of technologies in the Authentication and Access Management spaces[1] that *THE BANK* will not inherently be able to leverage with an in-house solution. *THE BANK* should deploy a technology that will meet the requirements of today while preparing for the efficiencies that converging technologies will provide in the mid-term.

Vendor Solutions

There are a multitude of vendor products that provide differing levels of Extranet access management and integration. Diagram 1 below illustrates the typical architecture and flow for a vendor solution.

[1] Gartner, Technology Overview DPRO-99280 by Ant Allan, December 6, 2002

Example of Successful Document Retrieval

In this example, a policy has been created which specificies:
"If the user is a member of Cost Center 1010, allow access"

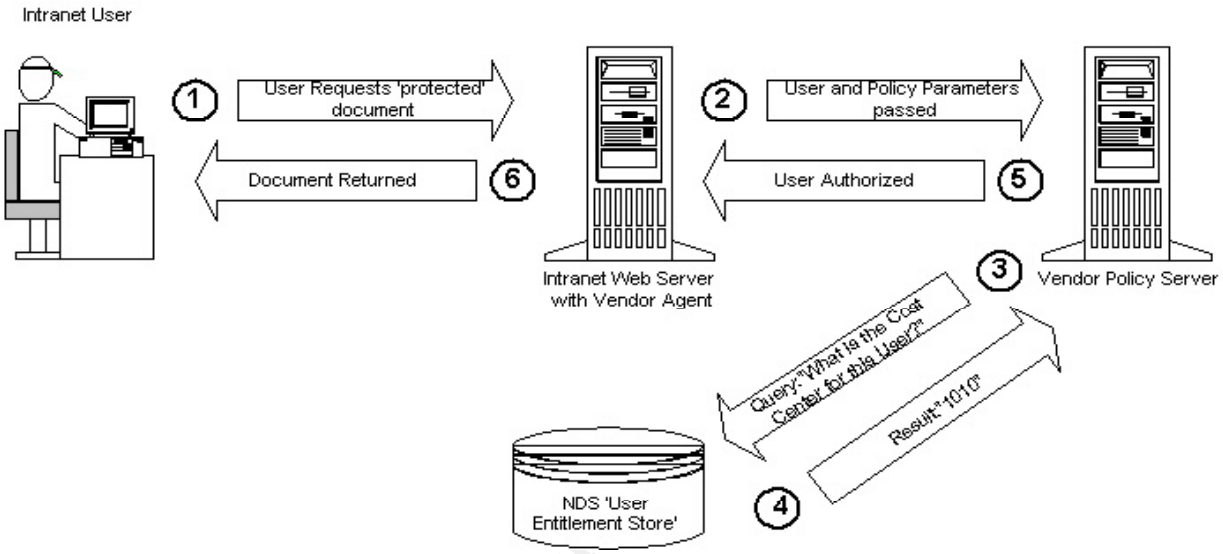

Diagram 1

Following are the major companies competing in the Extranet Access Management market:

Market Leaders
- Netegrity
- IBM
- Oblix

2nd Tier
- CA (Computer Associates)
- Novell
- RSA Security
- Entrust
- Open Network Technologies

Netegrity was named in a Gartner Research Report[2] as being one of three market leaders in the Intranet Access Management market space and ranks highest in their 'Magic Quadrant'. The other two companies named as a market leaders are IBM and Oblix. Novell is listed as a challenger well postured to excel in the Extranet Access Management space. CA has filled in a robust suite

[2] Gartner, Research Note M-18-9644 by J. Pescatore and R. Wagner, January 8, 2003

of offerings since the Gartner research note. RSA Security, Entrust and Open Network Technologies were found by Gartner to be moving forward in the Extranet Access Management space but displayed technical, financial or structural flaws not found in the market leaders. Gartner also named Entegrity, Baltimore Technologies, Wipro and Vasco as niche players in the market. None of those niches appear to have direct correlation to *THE BANK*'s businesses.

Table 2 shows the major companies competing in this software market space.

Table 2, Major Competitors

Company	Software
Netegrity	SiteMinder 5.5
IBM	Policy Director
Novell	SecureAccess 1.5
Computer Associates	ETrust WebAccess
RSA Security	Sentry CA 3.6
Entrust	GetAccess 7.0
Oblix	NetPoint 6
Open Network Technologies	DirectorySmart
Entegrity	AssureAccess
Baltimore Technologies	SelectAccess

Vendor Considerations

There is substantial overlap in the multitude of vendors providing various features and functionality desired for a broader solution for *THE BANK*. It is easy to become overwhelmed trying to compare various vendors against the value that they could add in addition to or instead of the primary goals of the project. A comparison of vendor capabilities is provided on Diagram 1.

Diagram 1

				Entitlement Store/Directory Interfaces								
Vendor	**Product/Release**	**Initial Cost for 10K licenses**	**URL level Access Control**	**LDAP**	**ODBC**	**Active Directory**	**NDS**	**ACF2**	**Architecture**	**IIS**	**J2EE**	**JRUN**
Netegrity	SiteMinder 5.5	$126,000	Y	Y	Y	Y	Y	Y	View	Y	Y	Y
IBM	Policy Director		Y	Y	N	Y	N	Y	View	Y	Y	
Novell	SecureAccess 1.5	$1,390,000	N	Y	N	Y	Y	N	View	Y		N
RSA Security	Sentry CA 3.6		Y	Y	N	Y	N	N	View	Y	N	N
Entrust	GetAccess 7.0		Y	Y	?	Y	Y	Y	View	Y	N	N
Oblix	NetPoint 6	$150,000	Y	Y	Y	Y	Y	N	View	Y	Y	Y
Open Network	DirectorySmart	$125,000	Y	Y	Y	Y	Y	N	View	Y	Y	N
Entegrity	AssureAccess	$45,000	N	Y	?	Y	?	?	View	Y	N	N
Baltimore Tech	SelectAccess	$200,000	Y	Y	?	?	Y	?	View	Y	N	N
Vasco	VacMan Server 6.0		N	Y	Y	Y	N	N	View	Y	N	N

As Diagram 1 shows, many of the leading vendors could provide a solution that would work in *THE BANK's* environment. This requires that we focus on viable, market leading vendors that have a proven solution to our immediate need of securing content on the Intranet as well as an existing relationship with THE BANK.

This brings the short list to Netegrity, IBM, Oblix, Novell and Computer Associates

Table 3 is a comparison of the strengths and weaknesses of these 'short list' vendors.

Table 3, 'Short List' Vendor Comparisons

Vendor	Strengths	Weaknesses
Netegrity	Leader in market share and 'mind share' for Intranet Access Management	Posted a $66 mil loss for the Q3/2002 which includes a 57 mil write off from bad acquisition.
	Rated market leader by Gartner	Laid off 20% of its workforce in October 2002, from the above acquisition.
	Has interfaces into all existing user entitlement stores, including ACF2, NDS and Active Directory	
	A specific-use Netegrity SiteMinder implementation is in place at *THE BANK*	
	THE BANK has acquired 100K licenses from a recent merger.	
IBM	Rated market leader by Gartner	Implementation rumored to require many pieces of proprietary software
	Touted as 'best positioned to own the identity management market'[3]	Still completing the integration of products from various acquisitions
	IBM Websphere product already in use at *THE BANK*	
Oblix	Rated as 'market leader' by Gartner[4]	
	Oblix 'Netpoint' product currently in use at *THE BANK*	
Novell	Rated as a 'market challenger' by Gartner	Limited support for non-Novell user entitlement stores

[3] Information Security Magazine, 'The Influence List' by Andrew Briney, November 2002
[4] Gartner Research Note M-18-9644, J. Pescatore, January 8, 2003

	Several Novell security products (Border Manager, Proxy Server) already in use at *THE BANK*	Long-term viability of company uncertain
Computer Associates	Purchased a solid Web Access control product.	Content Access component of 'eTrust' suite just released
	Several CA products already in use at *THE BANK*, specifically ACF2 for Host access control	Gartner has dropped CA out of the 'Magic Quadrant' at this time[5]
		CA products historically difficult to install at *THE BANK*

Table 3, continued

Recommendation

Three facts make Netegrity the most attractive choice:

1) Unquestioned dominance in market share and installed base of the Extranet Access Management market.
2) Licenses available through the *COMPANY X* merger as well as *COMPANY X's* subscription to all required modules. Based on conversion strategy, this could effectively eliminate the one-time software costs for this initiative.
3) *COMPANY X* completed a similar project within the last year and holds substantial expertise in this suite of products as well in-place hardware.

Implementation Approach

To achieve some measurable successes and integrate access control and identity management into *THE BANK's* environment, the implementation should be broken into four phases with specific deliverables and milestones in each phase.

Phase 1, Intranet Content Security

1) Timeframe – completed within 6 months.
2) Scope - Enhancing FileNet publishing usage by securing content with Netegrity SiteMinder. This will include procedural changes at both technical and non-technical level. The existing mechanisms of securing content user by user will be replaced with rules and policies that leverage existing directory information such as cost center and company. Additionally, delegated management will be established allowing a local administrator to add and remove user access where appropriate. While creating a cultural shift in some business areas, the benefits will be substantial the in terms of reduced turnaround time and reduced volume of access request the to centralized Access Control group.

Phase 2, Application Access Control

1) Timeframe – completed with 1 year.

2) Scope - Provide application access control for all internal Intranet applications. This will provide a consistent and scalable authentication model, replacing the dissimilar methods used currently by different development areas. This will additionally provide a common login screen, freeing the development teams from coding security. Existing applications can be 'retrofitted' as they come for maintenance and enhancement. To insure compliance to this standard application authentication methodology, a Standard will need to be passed to enforce its use throughout the enterprise.

Phase 3, Single Sign On

1) Timeframe – completed within 2 years
2) Scope – Provide a single login to multiple internal and external applications to internal and external customers. Internal groups such as Mortgage maintain Ids and passwords on more than a dozen systems (Infocus, Corepoint, Fundtech, etc.) today. Likewise, external business customers often have four or more Ids related to THE BANK's systems (Web Business Banking, Web Infocus, Construction Lending, Fidelity, etc.). This phase will improve security, efficiency and enhance the user experience.

Phase 4, User Rights Provisioning

1) Timeframe - completed within 3 years
2) Scope – The continued growth of *THE BANK* to more than 15,000 employees necessitates the implementation of provisioning system [5]. While the most difficult phase to implement the long term reduction in Access Control and Help Desk FTE will provide tangible ROI[6]. Additionally, the ability to quickly remove all user rights will reduce overall risk to the organization.

Costs

Based on the above recommendation and license transferal from COMPANY X, the largest cost would likely be internal FTE expenses. Professional Services cost may be reduced if key *COMPANY X* employees are engaged. The primary technical resources from the *COMPANY X* project team have a termination date of October.

Table 4 contains the estimated Costs for the project.

Table 4, Estimated Costs

Item	One-Time Cost	Recurring Annual Cost (Maintenance Contract)
Netegrity SiteMinder (50K Extranet Users)	$0*	$53,081

[5] 'Identity Checkpoint', by George Hume, Information Week, January 20th, 2002
[6] See Attachment B which is an ROI analysis provided by Netegrity

Hardware	Between $0 and $80K depending on re-use considerations	N/a
Professional Services	**$40K****	N/a
Internal FTE costs	TBD	.1 System Administration (NCS) .1 Policy Creation .25 Access Control
Training costs	$10,000 (2 people, 2 classes)	
Additional Software	10K	

Table 4, Estimated Costs, continued

*Expected cost as *COMPANY X* has 100K licenses currently in-force
** This could be less if existing *COMPANY X* expertise could be used

Potential Savings

To provide some financial motivation for commencing this project, a 'thumbnail' analysis of potential savings for the first two phases of the project have been performed. The figures represent an averaging of work effort based on previous projects over the past year. Clearly, some of the eliminated FTE costs will be transferred to the Information Security area and the Access Control group specifically. It is anticipated, however, that significant efficiencies will be achieved, reducing the overall FTE costs.

Phases 3 and 4 (single sign on and provisioning) are quantified on Attachment B. This is an ROI analysis provided by the vendor, so probably a little generous on the rate of return.

Table 5 contains some potential savings for phases 1 and 2 of the project.

Table 5 Potential Savings

Item	**Formula**	**Typical Yearly Savings**
Reduced FTE costs to secure Intranet content	150 Hours/project x $46/hour x Number of projects	150 x 46 x 7 = **$48,300**
Reduced FTE costs for Web Development Group	120 Hours/project x $46/hour x Number of projects	120 x 46 x 6 = **$33,120**
Elimination of Oblix license maintenance	$30,000	**$30,000**
	Total yearly savings	**$111,420***

***There will be increased FTE expense in the Information Security department which is included in the 'Costs' section

Proof of Concept Pilot

To establish the validity of phase 1 of this proposal, a proof-of-concept was performed in the NCS Test Lab. What was accomplished was nearly identical to Diagram 1 on page 3, which involved establishing a Netegrity 'Policy Server' and placing the Netegrity 'Web Agent' on the Intranet Server. A policy was created to secure an arbitrary section of the Intranet. In this case, the NCS 'Knowledge Base' was chosen. Then a rule was generated that stated 'Allow access to anyone from Cost Center XXX, deny all others'. When the test user attempted to access the NCS Knowledge Base, they were queried for Login Id and Password. This provided three possible outcomes:

1) The user was authenticated to the NDS directory and authorized via the Netegrity rule and the 'Knowledge Base' page was returned.
2) The user authenticated to NDS but was unauthorized to access the document and redirected to another page
3) The user was not authenticated to NDS and a message to that effect was provided.

This was an extremely simple proof-of-concept, but had real-world applicability. Most of the effort for this was in establishing the Policy server and Web agent. Due to the rudimentary test chosen, the rule generation was simple. That is certainly not to imply that the creation of the policies, rules and groups to support Extranet Access Management will be trivial. In-house expertise will certainly need to be established and substantial up-front work will be required. The expected mid-term benefits will be consistent, scalable and flexible Extranet Access Management with potential for even greater efficiencies in long term.

Summary

While the four phases of the project will require more than three years to implement and will likely range into the middle six figures in FTE costs, this project will establish a security infrastructure that will allow *THE BANK* to align itself with organizations of similar size. The return on investment will be tangible, but often difficult to quantify. Perhaps more important but not included on an ROI analysis is the value of centrally managing all access and controlling risk. The scrutiny of the Federal regulators has increased with every increase in *THE BANK'*s size. This security infrastructure will also provide verifiable access controls which *THE BANK* has repeatedly been found to be deficient in during Federal audits.

Attachment A

10K User Intranet

Direct Investments	Year 1	Year 2	Year 3	Total
Hardware	$ 40,950	$ 4,450	$ 4,628	**$ 50,029**
Software	$ 66,192	$ 9,909	$ 9,974	**$ 86,075**
Labor	$ 408,255	$ 123,208	$ 128,137	**$ 659,599**
Total	**$ 515,397**	**$ 137,568**	**$ 142,739**	
Cumulative	**$ 515,397**	**$ 652,964**	**$ 795,704**	
Net Present Value	**$ 772,215**			

Direct Benefits	Year 1	Year 2	Year 3	Total
Security Administration	$ 143,766	$ 168,206	$ 201,368	**$ 513,340**
Help Desk	$ 106,518	$ 124,626	$ 149,197	**$ 380,341**
Development	$ 560,000	$ 655,200	$ 784,376	**$ 1,999,576**
Indirect Benefits				
Increased Productivity	$ -	$ -	$ -	**$ -**
Total	**$ 810,284**	**$ 948,032**	**$ 1,134,942**	
Cumulative	**$ 810,284**	**$ 1,758,316**	**$ 2,893,257**	
Net Present Value	**$ 2,714,748**			

Return on Investment:

ROI over 3 years	**164%**
Dollars Saved	**$ 1,276,308**
Payback Period (in years)	**1.13**
Internal Rate of Return	**61%**
Internal Hurdle Rate	**25%**
Total Hours Saved for Security Administration	**4,853**
Total Hours Saved for Help Desk	**3,596**

List of References

1) Gartner, Technology Overview DPRO-99280 by Ant Allan, December 6, 2002
2) Gartner, Research Note M-18-9644 by J. Pescatore and R. Wagner, January 8, 2003
3) 'The Influence List', by Andrew Briney, Information Security Magazine, November 2002
4) 'Identity Checkpoint', by George Hume, Information Week, January 20th, 2002
5) Netegrity ROI analysis spreadsheet excerpt . ovided by Netegrity
6) Vendor Websites, enumerated in Diagram 1, on page 6