SANDIA REPORT

SAND2004-3254
Unlimited Release
Printed February 2005

Policy Based Network Management

State of the Industry and Desired Functionality for the Enterprise Network

Security Policy / Testing Technology Evaluation

Curtis M. Keliiaa, Lawrence F. Tolendino,
Martha J. Ernest, Michael A. Rios, Jeffrey L. Taylor,
Timothy L. MacAlpine, Edward J. Klaus, Christine A. Morgan

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2004-3254
Unlimited Release
Printed February 2005

Policy Based Network Management

State of the Industry and Desired Functionality for the Enterprise Network

Security Policy / Testing Technology Evaluation

Curtis M. Keliiaa
Advanced Networking Integration Department

Jeffrey L. Taylor
Cyber Monitoring and Analysis Department

Lawrence F. Tolendino, Michael A. Rios
Network System Design and Implementation Department

Timothy L. MacAlpine
Cyber Security Technologies Department

Martha J. Ernest, Christine A. Morgan
Cyber Enterprise Management and Process Integration Department

Edward J. Klaus
Systems Analysis and Trouble Resolution Department

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0788

ABSTRACT

Policy-based network management (PBNM) uses policy-driven automation to manage complex enterprise and service provider networks. Such management is strongly supported by industry standards, state of the art technologies and vendor product offerings. We present a case for the use of PBNM and related technologies for end-to-end service delivery. We provide a definition of PBNM terms, a discussion of how such management should function and the current state of the industry. We include recommendations for continued work that would allow for PBNM to be put in place over the next five years in the unclassified environment.

TRADEMARKS

Application Aware Networks is a trademark of AT&T Corporation
Intelliden R-Series Software is a trademark of Intelliden Corporation
Secure Mobile Architecture is a trademark of Boeing Corporation
CiscoWorks is a trademark of Cisco Systems Inc.
CiscoWorks QoS Policy Manager is a trademark of Cisco Systems Inc.
CiscoWorks LAN Management Solution is a trademark of Cisco Systems Inc.
CiscoWorks Small Network Management Solution is a trademark of Cisco Systems Inc.
CiscoWorks Routed WAN Management Solution is a trademark of Cisco Systems Inc.
CiscoWorks IP Telephony Environment Monitor is a trademark of Cisco Systems Inc.
CiscoWorks Voice Manager is a trademark of Cisco Systems Inc.
CiscoWorks VPN/Security Management Solution is a trademark of Cisco Systems Inc.
IP Solutions Center Security Policy Manager is a trademark of Cisco Systems Inc.
Identity based network services (IBNS) is a trademark of Cisco Systems Inc.
NetSight Atlas Policy Manager is a trademark of Enterasys Corporation
User Personalized Network is a trademark of Enterasys Corporation
SUSE LINUX is a trademark of Novell Corporation
Netware is a trademark of Novell Corporation
Novell eDirectory is a trademark of Novell Corporation
Sun Java Enterprise System is a trademark of Sun Microsystems Corporation
Java 2 Enterprise Edition (J2EE) is a trademark of Sun Microsystems Corporation
ColdFusion is a trademark of Macromedia Corporation
Active Directory Services is a trademark of Microsoft Corporation
Action Request System is a trademark of Remedy Corporation
Visionael is a trademark of Visionael Corporation
NetCool is a trademark of Micromuse Corporation
HP OpenView is a trademark of Hewlett-Packard Company
IBM is a trademark of IBM Corporation

ACKNOWLEDGEMENTS

Special Thanks to Anne Van Arsdall for her encouragement and support.

CONTENTS

[This Page Intentionally Left Blank]

INTRODUCTION

Policy-based network management (PBNM) uses policy-driven automation to manage complex enterprise and service provider networks. Sandia has existing electronic processes that perform the functions of account management and policy-based networking, but not with the tightly integrated automation and fine-grained control that newer technologies offer. The contributing staff members believe it is time to look at how newer technologies like PBNM can help make the growing complexity of our enterprise environment more manageable. We recommend the development of a standards-based automated configuration/change management capability that can be tightly integrated with cyber enterprise management (CEM). This capability must allow multi-vendor configuration control with demonstrated operational support system interoperability.

There is a long history of failure in the industry's pursuit of automated management solutions. Only recently have technologies and standards matured to the level needed for dynamic network management to succeed. One of the hot technology areas involves the use of policies, derived from business rules, to enable automated management of the enterprise with a business-centric view. This report discusses how PBNM and related technologies, such as identity management (IdM) and service oriented architecture (SOA) can be used for this capability in support of end-to-end service delivery.

Industry wide vendor use of directory services and the extensible markup language (XML) provide a foundation for more reliable and functional networks. Directory services are designed to contain information about people, policies and resources and have become strategic to enterprise management systems such as PBNM and IdM. These technologies offer strong security and authentication as well as the capability to manage users, groups, policies and roles. In response, network operating system vendors have delivered directory-enabled solutions that include Sun Java Enterprise System, Novell eDirectory (SUSE LINUX and Netware) and Microsoft Active Directory. Intelliden Corporation offers a directory-enabled solution for network management. Directory service architecture, process workflow and business-rule-based configuration control are provided by the Intelliden solution.

Although a full exploration of policy management is beyond the scope of this report, an important element is to approach development with an eye to how business-oriented policy can be distilled into implementable network management rules. At the highest level, policy management must be considered from a business perspective. Policy definition begins with an understanding of why we do business, how we do business, and with whom we do business. This understanding is fundamental to a managed policy framework for the enterprise network.

An integration model that includes XML, the lightweight directory access protocol (LDAP), the simple object access protocol (SOAP), and Java provides the "plumbing" for distributed communication. This framework facilitates coordinated account, entitlement and network service provisioning when utilized as an "enterprise service bus" to enhance communication between application, computing, network and operational support systems. Attributes from each of these functional areas can be shared for integrated process control. The enterprise service bus also facilitates event correlation, where events can be used to trigger appropriate actions, thus providing dynamic response to critical situations.

This report affirms the immediate gains that can be reached with a PBNM capability that is closely aligned with IdM. We discuss the technology evaluation, conceptual design and deployment of an enterprise PBNM strategy. We present an explanation of the terms used in PBNM, then a description of desired functionality and; state of the industry, followed by findings and recommendations for continued progress.

Automated Network Device Management
Automated network device management consists of the capability to control network device configuration by managing the changing and or maintaining the state of network devices through process-controlled configuration management.

Consumer
For the purpose of this report a consumer utilizes a network service, resource or function. A consumer may be an individual network user, an application, or a network service that is dependent upon another network service.

Common Information Model
The Distributed Management Task Force common information model (CIM)[1] provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions. CIM is comprised of a specification and a schema. The schema provides the actual model descriptions, while the specification defines the details for integration with other management models.

Customer Facing Services
The TeleManagement Forum's[2] (TMF) directory-enabled networking new-generation (DEN-ng) information model refers to packaged network services that constitute a product as customer-facing services. Product service bundles are delivered in various service-levels, such as platinum, gold, silver and bronze. Customer-facing services are services that are visible to the end user (i.e. virtual private networks (VPN), video conferencing and voice over IP (VoIP)). Customer-facing services are supported by resource-facing services that are transparent to the end user (i.e. network traffic control technologies).

Directory Enabled Networking
The Distributed Management Task Force (DMTF) directory enabled networks (DEN)[3] initiative is designed to provide the building blocks for more intelligent management by mapping concepts from CIM (such as systems, services and policies) to a directory, and integrating this information with other web based enterprise management (WBEM) elements in the management infrastructure. This facilitates end-to-end service delivery and supports distributed network-wide service creation, provisioning and management.

Directory Enabled Networking New Generation
DEN-ng (an extension of the original DMTF DEN standard) is being built under the auspices of the TMF Data Modeling Work Group. The DEN-ng policy model is a set of information models that are oriented towards business, system and implementation viewpoints. The DEN-ng information model focuses on network elements and services. DEN-ng defines policy models to accommodate different domains. For example, the service model defines customer-facing services and resource-facing services

[1] http://www.dmtf.org/standards/cim

[2] http://www.tmforum.org

[3] http://www.dmtf.org/standards/den

and the resource model defines logical and physical resources. The primary building blocks of DEN-ng include an information model, policy language and a data dictionary.

Enterprise Policy Management System
For the purpose of this report, the enterprise policy-management system describes distributed policy management, which includes disparate policy domains, policy-domain elements and policy sub-systems with the capability of consistent policy enforcement. For example, the Sandia unclassified network represents a policy domain, where an identity policy repository and a PBNM network configuration repository are domain elements, each with separate policy sub-systems.

Enterprise Service Bus
For the purpose of this report, the enterprise service bus comprises event, messaging and service registration/lookup functionality. The enterprise service bus supports distributed system communication for the application, computing, network and operational support system components of an enterprise network. The enterprise service bus facilitates attribute sharing and event correlation through communication based on standard interfaces (i.e. LDAP, XML, SOAP and Java).

Identity-Based Policy Enforcement
Identity-based policy enforcement is a value-add concept that joins in practice the fundamental relationship between identity and policy. Identity-based policy enforcement practical implementation is based on common baseline technologies that support both IdM and PBNM. This common framework makes possible the alignment of IdM and PBNM service architectures.

Identity Information Repository
An identity information repository is a data store for identity information. For the purpose of this report it references a central collection point for identity information. For example, an enterprise directory service can serve as the identity information repository for an IdM implementation.

New Generation Operations Systems and Software
The TMF new generation operations systems and software (NGOSS) program delivers a framework for operational and business support systems. NGOSS solutions are designed to easily integrate with other systems, improving software re-use and operational flexibility.

Policy
For the purpose of this report a policy is a business rule-based statement, which defines the required response (action) to an event or sequence of events to enforce behavioral or functional compliance. Policy enforcement is based on the triplet of event, condition and action. A policy falls into one of three categories: security policy utilized for access-control, detection, alarm and notification; quality of service (QoS) policy utilized for network traffic management and policing; operational policy utilized for workflow, approval and process control.

In the context of DEN-ng, policy as defined by Strassner[4] "is a set of rules that are used to manage and control the changing and or maintaining the state of one or more managed objects".

Policy Based Network Management
Policy based network management (PBNM) as defined by Strassner "is a way to define business needs and ensure that the network provides the services that its clients require". The TeleManagement

[4] John Strassner, Policy Based Network Management, Morgan Kaufmann Publishers, Copyright 2004, Elsevier (USA)

Forum SID and DEN-ng information models provide the PBNM methods of business driven network device configuration.

Policy Continuum
A policy continuum permits policy to be expressed from different views. For example, the DEN-ng information model defines business, system, network, device and instance levels of policy abstraction. Each level uses appropriate policy terminology for specific purpose. The policy continuum model establishes policy translation through the use of an accompanying policy-language continuum. This permits consistent policy expression, as policy moves from one policy view to the next, while accommodating view specific syntax.

Policy Decision Point (PDP)
The policy decision point is the arbitration component for policy evaluation, which evaluates a state or condition to determine if a policy enforcement action is required.

Policy Enforcement Point (PEP)
For the purpose of this report a policy enforcement point is a network device, such as a router or switch, where policy is enforced (through dynamic configuration changes to access control lists, priority queues or other parameters) as directed by the policy decision point.

Policy Management Authority
The policy management authority[5] is an entity such as a person or application that produces electronic policy representations through a policy console, interpreter or other tool.

Policy Management Console
The policy management console[6] is the workstation and interface from which policies are managed.

Policy Management Tool
The policy management tool is the server or host where policy management software such as Intelliden R-Series software, Enterasys NetSight Policy Manager or Cisco Quality Policy Manager resides.

Policy Information Repository
A policy information repository is a data store for policy information. This data store may be application specific, operating system specific or an enterprise common repository. For the purpose of this report the policy information repository is a PBNM application specific directory service.

Policy Template
Policy templates facilitate interoperability between disparate repositories and for the purpose of this report are presented in two contexts. The first is a PBNM policy template, which provides a consistent policy format for PBNM system policy import and export. The second are XML based policy templates facilitating interoperability within the broader enterprise network.

Quality of Service
For the purpose of this report quality of service (QoS) references product service bundles, such as platinum, gold, silver and bronze, that consists of customer-facing network services, such as VPN,

---

[5] Burton Group Securing the Virtual Enterprise Network: Layered Defenses, Coordinated Policies, May 23, 2003

[6] Understanding Policy Based Networking, David Kosiur, John Wiley and Sons, 2001.

video conferencing and VoIP. QoS customer facing services are supported by resource facing services. The DEN-ng information model normalizes the variety of these QoS capabilities so that consistent implementation is possible.

Resource Facing Services
The TMF DEN-ng information model refers to behind the scenes network services as resource-facing services. Resource-facing services are the supporting cast for customer-facing services (i.e. VPN, video conferencing and VoIP). Resource-facing services comprise metering (aka rate limiting), policing, marking, queuing (buffering), traffic shaping and scheduling network traffic control technologies. These technologies include IP precedence, type of service (ToS), class of service (CoS), differentiated services (DiffServ) and integrated services (IntServ). Resource-facing services are transparent to the end user and provide underlying network functionality.

Role
A role represents an organizational, administrative or process function. For example, the functions and entitlements of a manager can be represented as a role. Similarly, PBNM introduces the concept of a role representing the functions of a network device such as a firewall, interior gateway or exterior gateway router, which then can be applied to devices fulfilling the role. A role has membership made up of parties (similar to group membership).

Service Oriented Architecture
Service oriented architecture (SOA) has emerged as a framework for web-based services. The SOA is comprised of a service provider, a service registry, and a service consumer. The intent of the SOA is for service providers to register available services with the service registry. Service consumers can then lookup available services by querying the service registry. When an available and desired service is located, the service consumer binds to the service provider for access (lease) to the published service. SOA is also applicable to the registration, publishing and binding of *network* services. When the consumer is finished using the service or when the lease has expired resources are released for other use. For example, service level agreements specify customer facing service levels to a variety of service consumers and SOA would facilitate the "find, bind, lease and release" of available services.

Shared Information and Data Model
The TMF shared information/data definitions and models (SID) consists of a set of object-oriented information and data models that represent concepts and entities in service provider and enterprise managed environments. The SID is used to describe the business, system, implementation and runtime descriptions of NGOSS policies, processes and data, all defined using the standard universal modeling language (UML) class models.

TeleManagement Forum
The TMF is an international standards organization responsible for the NGOSS architecture that includes the SID and DEN-ng information models and an enhanced telecom operations map (eTOM).

User
For the purpose of this report a user represents an authenticated network account with an active session and is a consumer of information and network resources.

[This Page Intentionally Left Blank]

DESIRED FUNCTIONALITY

This is an initial description of desired functionality and represents a starting point for the evaluation of PBNM technologies for the enterprise network. Functionality is discussed in three scenarios. The first addresses proof-of-concept functionality. Second, desired functionality is discussed in the context of network device management and CEM, with enterprise policy expression discussed as a precursor to future state functionality. Finally, discussion focuses on the future state, where IdM and PBNM are closely aligned for enhanced account, entitlement and network service provisioning. This report assumes directory-enabled PBNM and IdM capabilities coupled with XML-enabled automated network device management.

Proof of Concept Functionality

For the purpose of this evaluation a directory service is assumed as the repository for identity, policy and resource objects. User identity, policy and network resources will be logically associated within the directory service schema. The proof-of-concept stated goal of controlling the path between the requestor and the target is accomplished by means of an automated access-control list (ACL) configuration change. A user authentication event will be used to trigger the policy evaluation process. The change will then be rolled back at the end of the user's session.

The successful authentication of an LDAP identity serves as the trigger for policy assessment. For example, consider a visitor extranet, where machines are contained in a specific subnet. Initial access may be locked down to specific resources, such as a directory authentication server, until further access is authorized and enabled through policy enforcement. Similarly initial authentication may be localized to the same subnet. Two user access-control policy use cases are illustrated. User-A is permitted access to off-net resources hosted on another subnet, while User-B is denied access to off-net resources based on network access-control policy.

A positive policy condition results in a change (policy action) to the router interface ACL (the policy enforcement point). The change permits access to off-net resources based on the user-A identity. A negative policy condition results in no ACL change, assuming the ACL currently denies access for the user-B machine IP address. The step-by-step flow is as follows:

User-A successfully boots the computer and is presented with a directory service logon prompt. User-A successfully authenticates to the directory server. Successful authentication triggers associated policy assessment. Based on User-A's identity and policy association, network access to off-net resources is permitted. A policy enforcement action is enacted to permit access via a configuration change to the ACL to permit User-A's machine IP address access to the resource subnet. Access is permitted until User-A logs out causing the ACL to return to its original state.

User-B successfully boots the computer and is presented with a directory service logon prompt. User-B successfully authenticates to the directory server. Successful authentication triggers associated policy assessment. Based on User-B's identity and policy association, network access to off-net resources is denied. No further policy enforcement action is required (denial of the User-B machine IP address is assumed). The ACL is maintained at current state. Figure 1 illustrates the PBNM proof-of-concept identity-based policy enforcement.

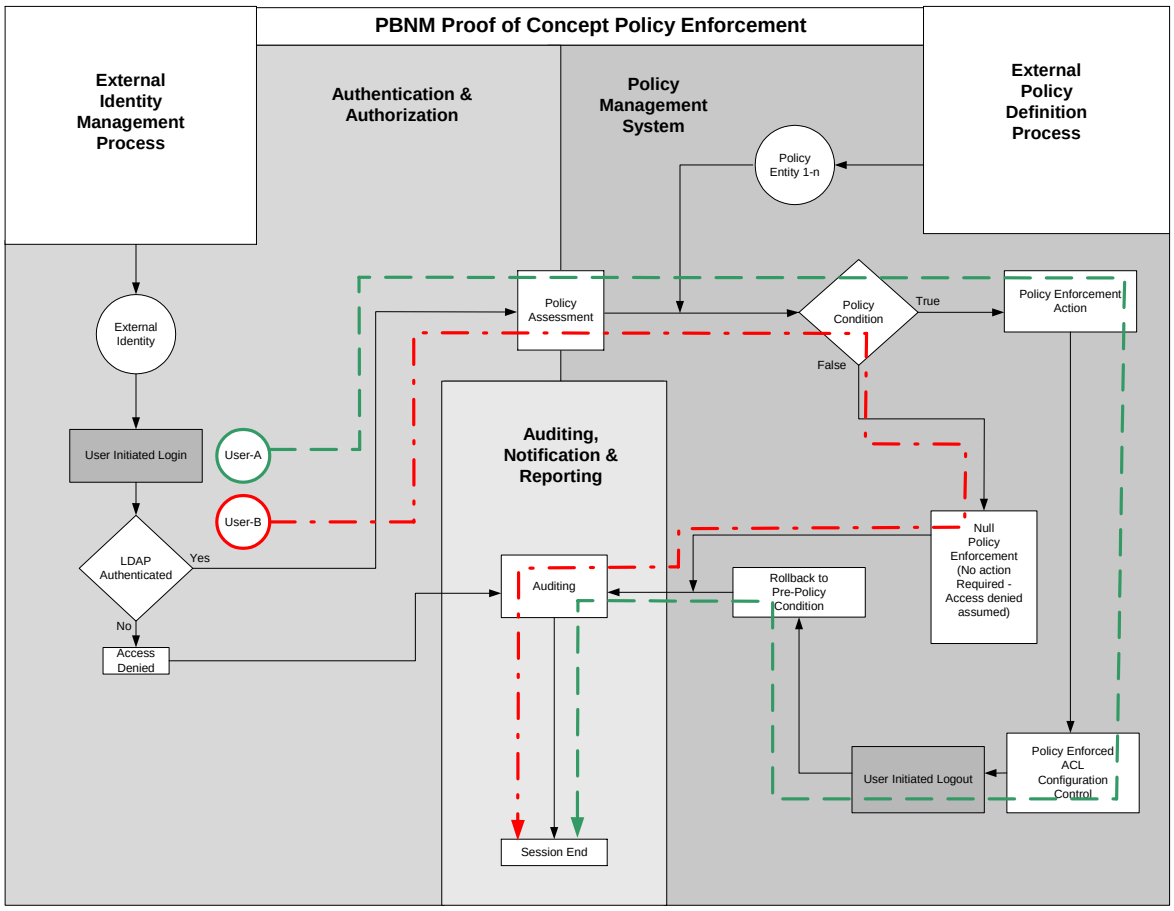

Figure 1. PBNM Proof of Concept Policy Enforcement

Baseline definition of specific business rules is needed for a PBNM solution. The proof-of-concept utilized CEM policy work to identify access factors and develop a generic proof-of-concept policy framework. This is an initial attempt at establishing primitive terms that may then be used to compose more complex policy statements. We started with the premise that identity attributes would be used to control access. As such, the path (open/closed) state is controlled to allow or disallow communication. The proof-of-concept was developed to express network specific access-control mechanisms. This test focuses on the network path factor. Note that per user management of network path through ACL's would have inherent limitations in a production setting that could result in performance and auditability difficulty by changing ACL's too frequently. In the production setting, this method of access-control would be limited to large aggregate groups such as employees, contractors or visitors. To further speculate on production deployment, the general trusted user population could have default access to network resources, thus reducing the frequency of ACL changes.

Element	Client	User	Use	Access Channel	Authorization	Path	Security Domain	Resource	Target
Element Attributes	Ownership (SNL, Other), Local, Remote, Platform (Unix, MS, Apple, Linux)	Authenticated user, Employee, Contractor (SBS, Offsite), Visitor (FN, Gov, Permanent, Temp)	Application (SSH, HTTP, SHTTP, Telnet, SMTP, LDAP, NBT, SMB, RPC, DCE, other)	Same LAN Different LAN, Dialin, VPN, Internet	Permit, Deny (CNTK, NCNTK)	Open, Closed	SON, DMZ, SRN, Remote	Platform (Unix, MS, Apple, Linux), OS (Sun, NT, W2K, W03, A9, AX, Redhat), File System (UNIX, FAT, NTFS, NFS	Data Description (Export Controlled Information, Official Use Only, etc.), Hosting repository (Local File System, LDAP, Database)
Path authorization permitted	SNL, Local, MS	Employee	NBT	VPN	Permit CNTK	Open	SRN	MS, W2K, NTFS	OUO, SQL
Path authorization denied	SNL, Remote, MS	Employee	NBT	VPN	Deny	Closed	SRN	MS, W2K, NTFS	OUO, SQL
Path same LAN permitted	SNL, Local, MS	Employee	LDAP	Same LAN	Permit CNTK	Open	SRN	Sun, Unix	OUO, LDAP
Path different LAN denied	SNL, Local, MS	Employee	LDAP	Different LAN	Permit CNTK	Closed	SRN	Sun, Unix	OUO, LDAP

Table 1. PBNM Proof of Concept Policy Framework

This framework is based on the following nine elements. The objective of the generic policy framework is to present a description of significant factors that exist in the progression from requested resource access to the granting of that access.

1. The client element represents location, asset and platform attributes that specify a client machine interpretation.
2. The user element represents an authenticated user with role and assignment attributes that specify a user-type.
3. The use element represents application and protocol attributes that specify a use context.
4. The access-channel element represents network entry or ingress attributes that specify an access-method.
5. The authorization element represents authorization and information-access attributes that specify an authorization context.
6. The path element represents an open or closed control method that specifies the permission or denial of traffic flow. Path element is independent of the technologies that lie between the client and resource elements.
7. The security-domain element represents a partitioned information environment where the destination resource resides. The security-domain element might be thought of as a common environment where similar resources or functionality reside.
8. The resource element represents platform, operating system and file system attributes that specify a resource machine interpretation. The resource element is where host-based protection mechanisms reside.
9. The target element represents data classification and host repository attributes that specify a data context.

To further theorize, these elements could be developed as directory-service schema extensions. These extended object types would contain attributes to be used with policy statements for policy enforcement.

Network Device Management And CEM Functionality

CEM requires a strong network device control capability that permits automated configuration/change management and the operational state of network devices to be managed. Change management must be in place that facilitate process controlled workflow and approval. This capability will facilitate design, review, and verification functionality and permit operational ISO 9001:2000 compliant processes to be modeled and automated in the PBNM system. Auditing and reporting are additional operational and security requirements. In the event of undesired results after implementing a change, the automated configuration/change management capability should provide a rollback function to back out the offending change.

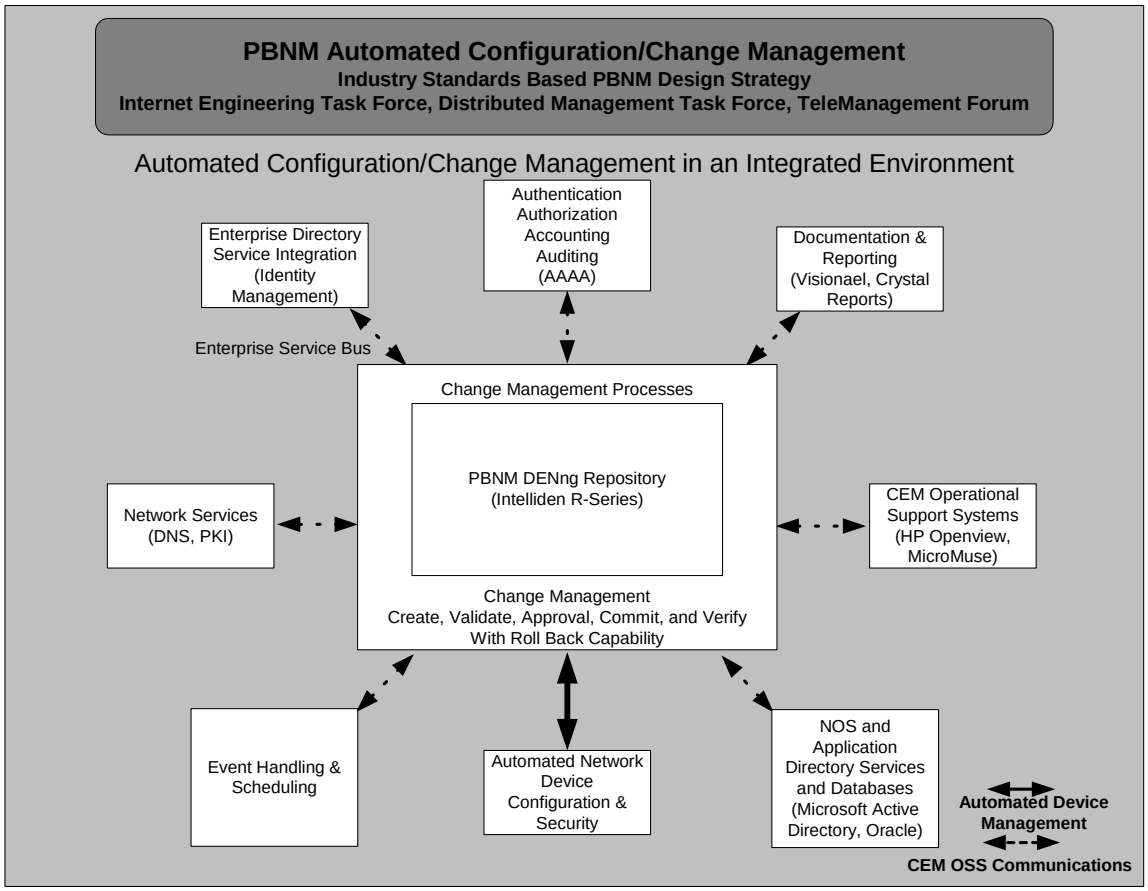

Figure 2. PBNM Automated Configuration/Change Management in an Integrated Environment

Figure 2 illustrates a PBNM automated network device configuration/change management capability in an integrated environment. CEM operational software and support communications are facilitated through an enterprise service bus using the transmission control protocol/Internet protocol (TCP/IP) standards. Note that the PBNM automated configuration/change management solution does not preclude manual intervention by authorized staff if warranted in an emergency situation. If such an occurrence were to happen, manual changes reflecting current state would need to be reconciled within the PBNM system.

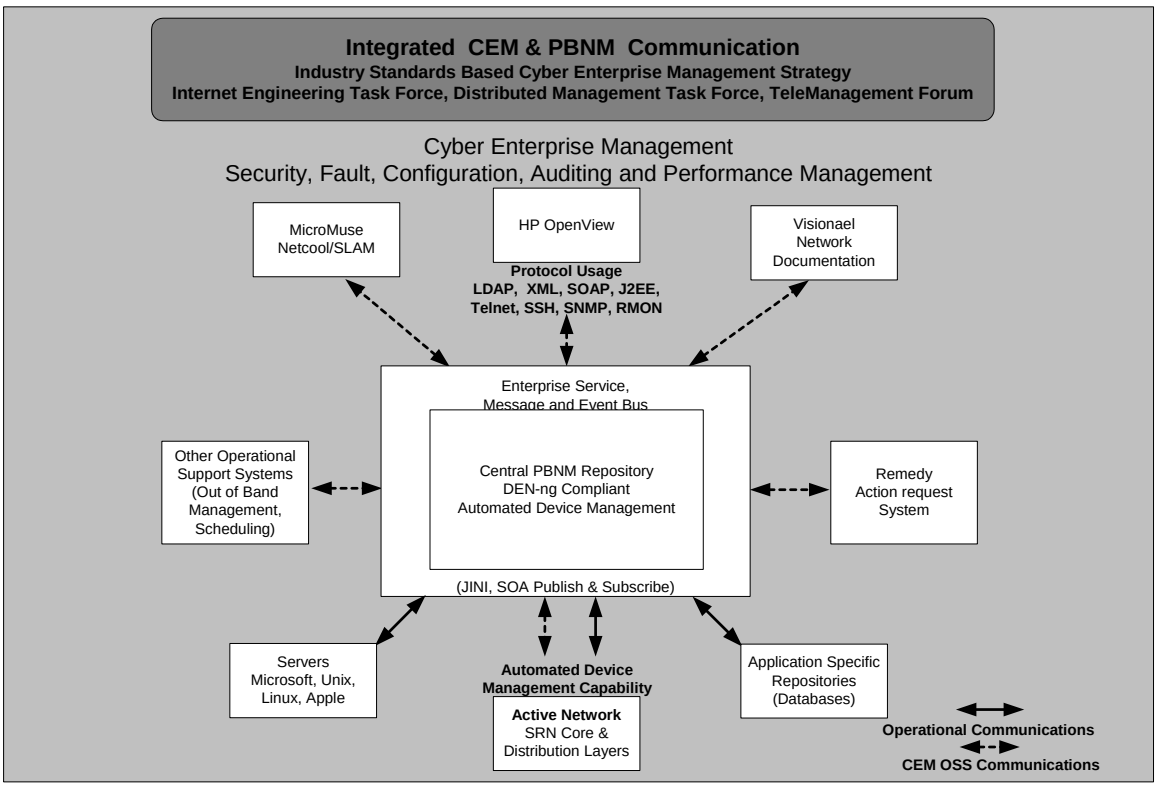

Figure 3. Integrated CEM & PBNM Communication

Figure 3 illustrates a CEM integrated operational support model. In addition to operational communication, the enterprise service bus functions to facilitate communication for all CEM components in support of the security, fault, configuration, auditing and performance (SFCAP) model (Note: in contrast to the industry FCAPS model). The enterprise service bus is the usage model for specific protocols and applications, including XML and LDAP that facilitate attribute sharing and event correlation. Note that corporate servers, applications and data repositories also connect to the enterprise service bus for operational communications.

The PBNM automated configuration/change management capability is integral to enterprise network management and contributes to the security, configuration, fault and auditing aspects of CEM. The Sandia integrated test environment (SITE) has been established as a testbed for proof-of-concept functional evaluation and the CEM development environment could be used for prototyping of integrated and automated configuration/change management functionality.

The proof-of-concept evaluation successfully demonstrated the feasibility of policy-based access-control security filters. Such functionality is supported by role-based access control (RBAC) for both users and devices. In the same sense, policies can be viewed as user oriented and device oriented. These two types of policy can be accommodated in the PBNM system for identity-based policy enforcement, which uses identity-attributes for access control to network resources. Two-factor authentication is an additional requirement. In support of this tactic, policy and authentication functionality will be developed, but will follow deployment of reliable automated configuration/change management, as policy-enforcement is dependent on the finite control of the automated configuration/change management capability.

Desired Future State Functionality

As a precursor to a discussion of future state functionality we introduce here the notion of enterprise policy expression. We have observed that methods for common policy expression are needed for consistency in the deployment of policy management throughout an enterprise network. This work begins with an understanding of policy from the business view. An audit of existing policy statements, and the context in which they apply, will yield the information necessary to quantify and categorize existing cyber policy implementation that can be translated into the PBNM system. The proof-of-concept policy framework only identifies simple factors and much more work is needed to develop consistent policy expression for an enterprise policy management system.

The development of XML policy templates help to provide a means of consistent policy expression in a heterogeneous environment. The XML standards provide a conduit to transport information content independently of presentation. XML and the associated suite of markup languages offer significant benefit to standardize information transport within the enterprise environment and with external collaborators. The development of common XML document definition types (DTD) or XML schema definition (XSD) would allow for example, human-resource data to be used with PBNM and IdM systems. The use of XML as a baseline technology is also compatible with web services SOA.

David Kosiur of the Burton Group has published works on policy-based networking that present the policy model illustrated in Figure 4. His representation is compatible with the DMTF CIM and DEN specifications. Figure 4 illustrates policy management system components so that policy management system operation can be visualized.

The PBNM proof-of-concept was conducted using the basic Kosiur model and the generic policy framework with simple policy statements (i.e. User-A is permitted access to off-net resources; User-B is denied access to off-net resources). The proof-of-concept successfully demonstrated the automated policy action of an ACL configuration change, triggered by the successful authentication of the appropriate user (User-A). The result was permissible access that was then revoked at the end of the user session (recall that policy enforcement is based on the triplet of event, condition and action).

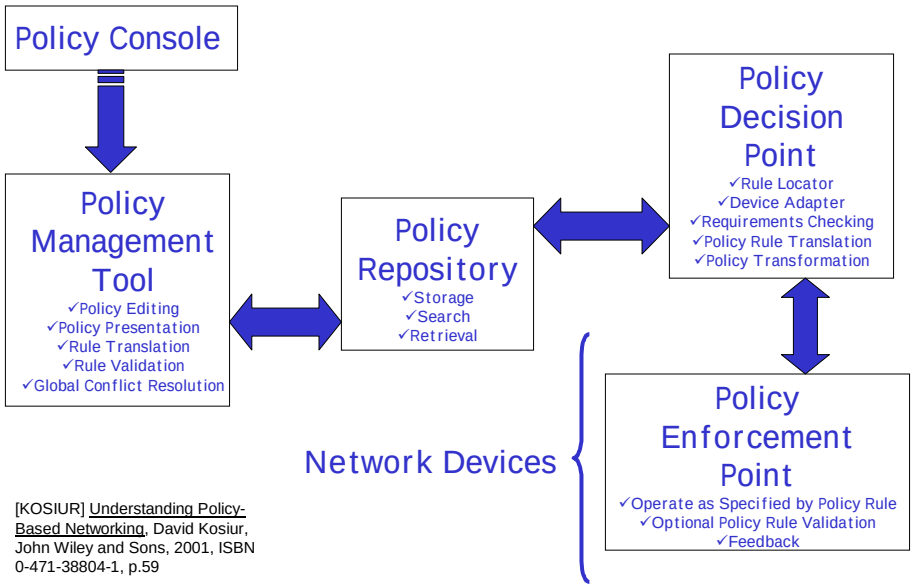

Figure 4. Policy-Based Network Reference Element Architecture

The policy console (policy management console) is the administration workstation from which policies are managed. The policy management tool is the server or host where policy management software resides. The policy repository is the datastore for policy specific information, commonly a directory service. The policy decision point is an arbitration software component that evaluates a state or condition to the target set of a policy. The policy enforcement point is the component where policy is enforced through an action such as a change in configuration.

There is some debate in the standards community concerning whether of the DMTF DEN specification is complete. At issue is how to accommodate policy enforcement. The TMF has developed the DEN-ng information model as a means to extend the original DEN for more complete definition. The DEN-ng information model introduces a finite state machine. State is used for managing the lifecycle of PBNM system changes and is based on maintaining current state and controlling the changing of state. Current state represents the current composition of elements within the managed system, which is maintained as a record for comparison and validation of changes. Once state has been changed, committed and verified, the current state is updated. The finite state machine also permits the lifecycle of cyber-policy to be managed and enables predictable rollback in the event undesired results.

Recent collaboration promises resolution to standard information model dispute. For example, the February 2004 release of RFC 3703, Policy Core Lightweight Directory Access Protocol (LDAP) Schema (PCLS) is under joint development of the IETF Policy Framework working group and the DMTF Policy working group. Listed authors include John Strassner, the inventor of DEN and DEN-ng.

The TMF has extended the DEN-ng information model with the notion that policy in expressed differently at different layers of a policy continuum. The TMF DEN-ng policy continuum, illustrated in Table 2, permits a rich policy framework. The policy continuum establishes policy translation through the use of an accompanying language continuum. This permits consistent policy expression and execution as policy moves from one policy view to the next, while accommodating view specific syntax.

POLICY CONTINUUM ↔				
Business View	System View	Network View	Device View	Instance View
Business Specific Terms – Service level agreements, processes and goals	Device and technology independent operation	Device independent and technology specific operation	Device and technology specific operation	Device specific (MIBs, CLI, etc.) Run time implementation
LANGUAGE CONTINUUM ↔				

Table 2. TeleManagement Forum Policy Continuum

Each view uses appropriate policy terminology for view specific purpose. For example, the business view uses business specific terms. Policy implementation from the system view, which is device and technology independent, gets more technology specific as policy progresses to the instance view. The network view is technology dependent but device independent and includes components such as an identity information repository and a policy information repository. The device view represents the programming model of a particular vendor and device, which is technology dependent and device dependent. Finally the instance view represents runtime implementation of a modification (i.e. change to a configuration parameter).

The building blocks for DEN-ng are an information model, a policy language, and a data dictionary. An information model provides the high-level abstraction needed for the PBNM system. A policy language provides the ability to express semantics at each layer of the policy continuum. A DEN-ng policy continuum and the accompanying language continuum provide the means in which policy is consistently applied from a business perspective to implementation. The data dictionary provides for a common definition of terms for various levels of policy expression. The data dictionary in effect defines synonyms and aliases so that policy expression is consistent at the various layers of policy continuum.

The TMF SID party model provides the framework for business entities and processes including customer, product and contract elements. DEN-ng defines network terminology that supports the business definitions of the SID information model. Network elements such as customer facing services, resource facing services and network devices are defined in the DEN-ng information model. In addition, resource and service policy models provide a means for consistent and predictable policy enforcement across disparate policy domains.

The Intelliden R-Series product is TMF SID and DEN-ng compatible. Detailed information regarding the TMF DEN-ng information model can be found in John Strassner's *Policy-Based Network Management, Solutions For The Next Generation*, referenced at the end of this report. However, it is important to note that the SID is focused on a detailed business perspective of all objects in the managed environment. The DEN-ng details network elements and services. In this context DEN-ng provides network detail into the SID.

Market research has revealed that the same baseline technologies support both IdM and PBNM. These technologies are now commonly deployed because of the need for provisioning of information services and secure collaboration. In addition, companies including Hewlett-Packard, Cisco, AT&T, Boeing and Intelliden have invested in automated configuration management based on PBNM technologies. Market drivers for this activity include compliance with legislation such as Graham-Leach-Bliley and the Health Insurance Portability and Accountability Act. Evaluation of these technologies indicates that an enterprise policy management system can be achieved in part with XML and directory-enabled products. A fully functional system would be highly integrated within the enterprise network environment, combining directory-enabled identity management with rule-based policy enforcement. In light of this integrated functionality, we use the term "identity-based policy enforcement" to underscore the fundamental relationship between identity and policy. Identity-based policy enforcement is a guiding principle for future state functionality. Figure 5 illustrates an operational identity and policy integration model.

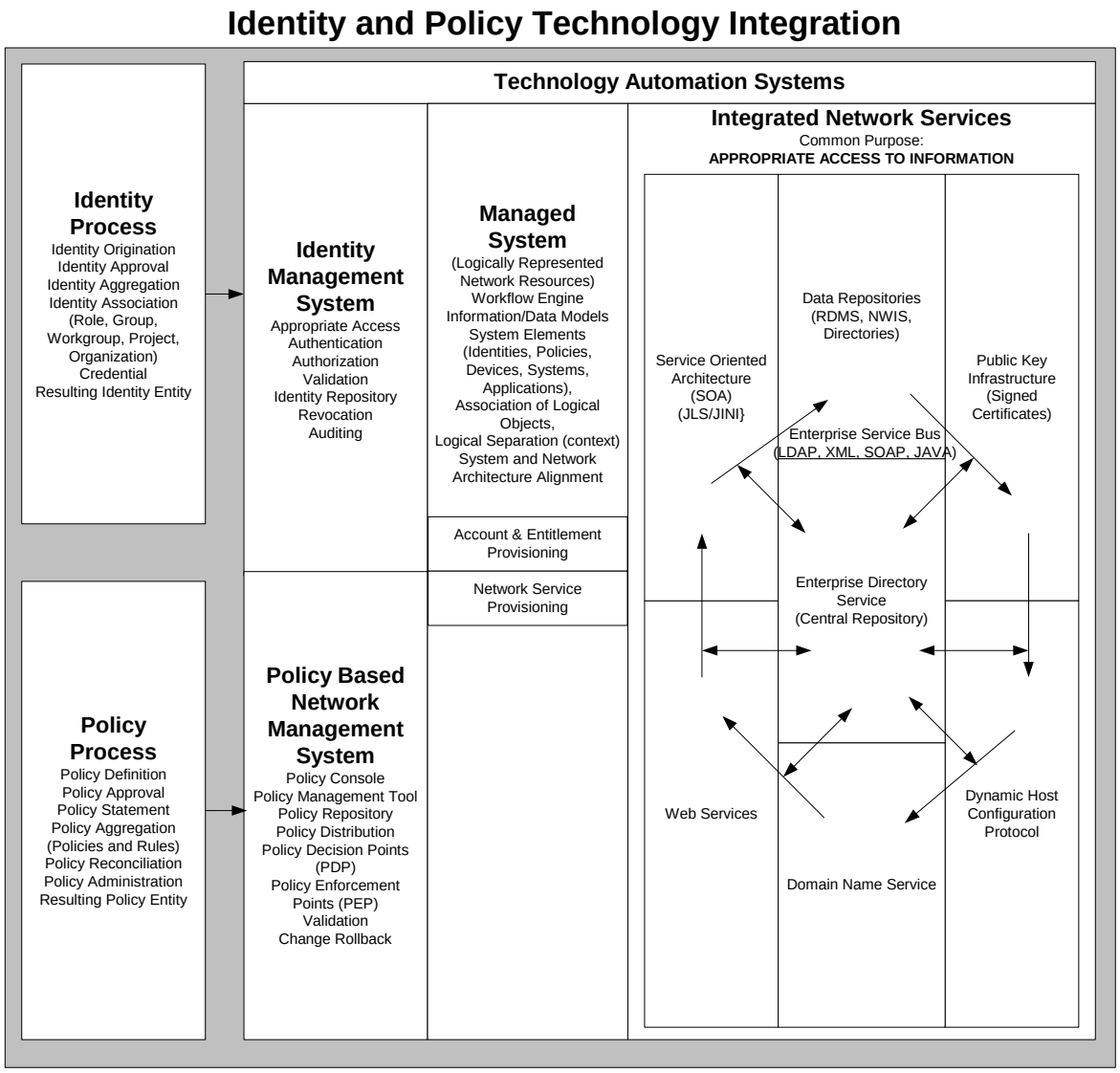

Figure 5. Identity and Policy Technology Integration

Identity-based policy enforcement integrates IdM and PBNM processes with auditing, notification and review functions to ensure auditable confidence. Well defined policies and processes are needed and considerable upfront effort is required. Sandia is using the ISO 9001/2000 standards to establish well-defined processes. PBNM embedded processes can be modeled from ISO compliant processes and coupled with a workflow engine, provide auditable and automated process control.

Identity and device RBAC is an example of the combined strength of IdM and PBNM integration. Role membership determines what a user or group of users are authorized do when a resource is accessed. DEN-ng introduces the concept of device functionality defined by roll membership as well. In this way administrative access to the device can be tailored through the combined use of user role and device role. RBAC serves as a means of enforcing entitlement policy to control who is allowed access to specific resources and which actions the user and resource are permitted to perform.

The logically managed system is the product of an information model[7], data models specific to databases or directories and elements (servers, applications, identities, roles, policies and network components) within the system. It is important to understand that the elements within the managed system are logically associated so that the management of relationships is possible. For example, the relationships of identity associated with policy, are in turn associated with resources such as router, server or application. The managed system also permits business elements, such as processes to be associated with network resources and managed with a high level of control that is not available with current implementations.

The integrated network services depicted in Figure 5 illustrate information flow, where each service is "cognizant" of its function and operates in concert with other network services. These services (i.e. enterprise directory service, public key infrastructure (PKI), dynamic host configuration protocol (DHCP) and domain name service (DNS)) communicate via the enterprise service bus. In addition, event correlation can be integrated with workflow and scheduling middleware such as Macromedia ColdFusion. The enterprise service bus permits the sharing of common information thereby reducing duplication and enhancing efficient network operations.

SOA provides a means to publish and subscribe available web and network services. To theorize on future state functionality, network services could be developed in the PBNM system, registered in an SOA registry and provisioned with embedded PBNM processes when a user or consumer of the service subscribes to the service-provider for lease of the service. Such a system offers the advantage of releasing network resources for other purposes when the user is finished with the service or the lease period expires. There is security benefit as well in that network resources are not left with open sessions or persistent connections.

Figure 6 illustrates a prototype enterprise policy management system that is based on the DEN-ng policy continuum to facilitate consistent policy enforcement. Also implied in Figure 6 is the tight integration of IdM and PBNM.

[7] The DMTF common information model (CIM) and directory enabled networks (DEN) or the TMF shared information data model (SID) and directory enabled networks new generation (DEN-ng)

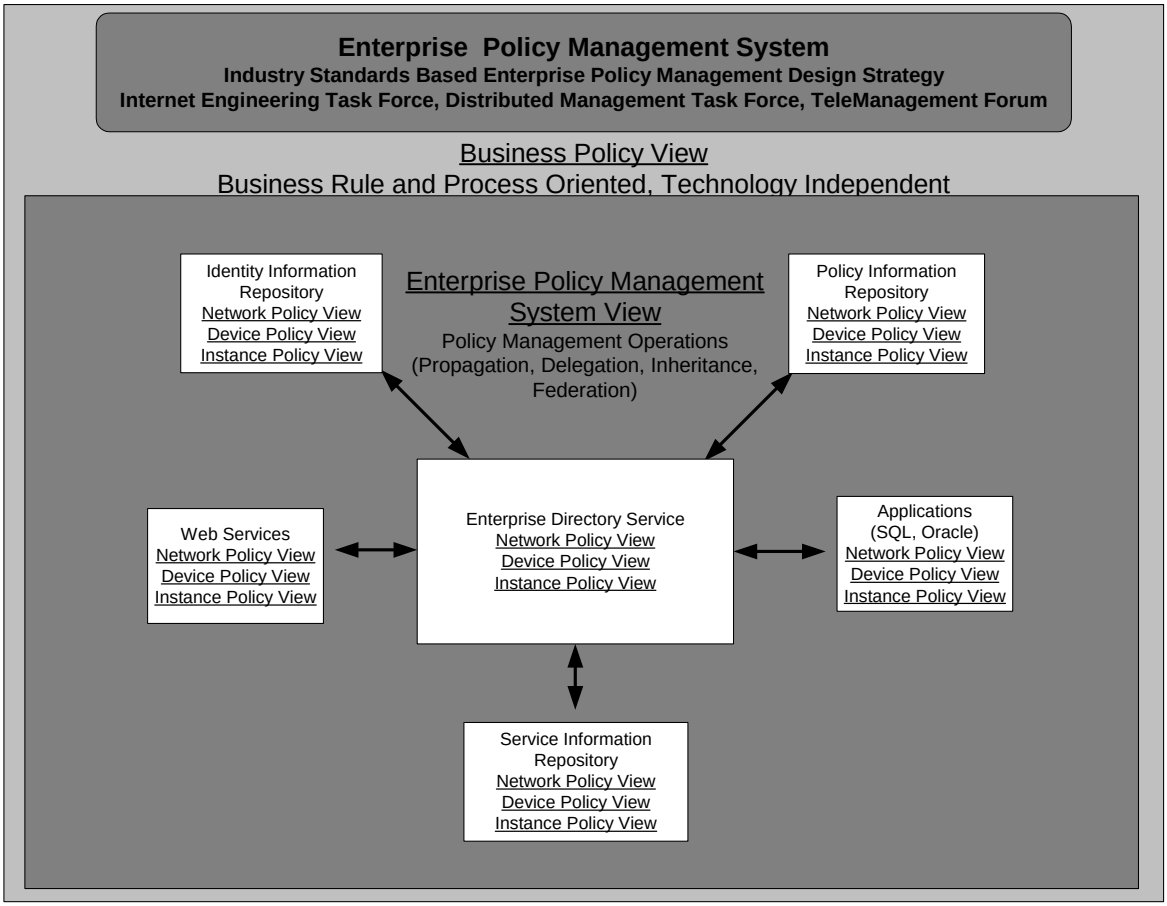

Figure 6. Enterprise Policy Management System

Each policy subsystem is considered to have a specific view and syntax. The policy subsystems are considered at the "Network View" of the policy continuum, as the subsystems are technology specific and device independent. For example, the policy information repository could maintain policy specific to network device configuration, whereas the identity information repository could maintain policy specific to user account management.

Figure 7 illustrates a possible future state in which industry standard protocols and interfaces are used for information exchange. Operational software and support systems communicate through the enterprise service bus and the application of SOA is applied to facilitate service delivery. Detailed discussion of the SOA is beyond the scope of this report, although it is important to note that SOA is critical to web service deployment and can also be utilized effectively for PBNM solutions.

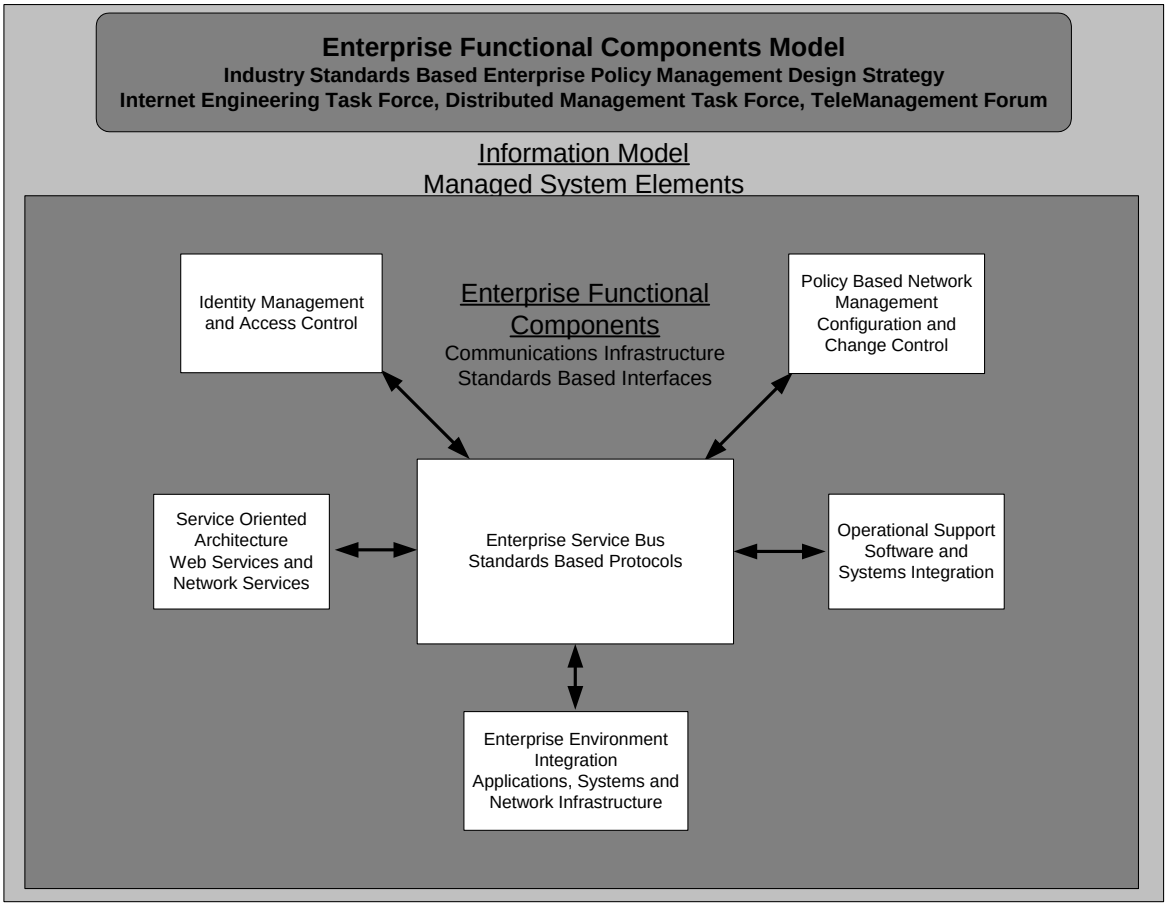

Figure 7. Enterprise Functional Components Model

The emphasis in Figure 7 is placed on standards based "plumbing" for information management. Without such information exchange capability, end-to-end service delivery cannot be fully realized. In such an integrated enterprise services environment, management information can be shared between the operational support, IdM, SOA and PBNM systems. The intent is to effectively integrate the application, computing, network and operational support system areas of the enterprise network. In this scenario coordinated account, entitlement and network service provisioning support on-demand network service delivery.

STATE OF THE INDUSTRY

The state of the industry is characterized by the evolution of standards and technologies that bring business policy to bear in the delivery of information services. This is evident in the wholesale adoption of directory services, XML and web-enabling technologies by both vendors and industry strategists. Established technologies such as Ethernet, TCP/IP, and directory services have been augmented by newer technologies, such as XML, and SOAP. This innovation with established technologies is the foundation of PBNM.

The concept of policy-based networking is not new but manual implementation is tedious and complex. Most policy management systems focus on a specific area of functionality such as security or QoS but rarely include the holistic association permitted by the standards-based information models. Older protocols (i.e. COPS, SNMP, DiffServ, and IntServ) remain as discrete mechanisms for network service delivery, but with PBNM the details are associated as related functions of one system.

Historically, security policy and quality of service (QoS) policy management have been considered as separate policy domains with specific tools unique to each. Most commercially available policy management systems offer only single vendor, single policy domain solutions. Many configuration management products offer advanced configuration management capability but lack the capability needed to integrate application, computing, network and operational support system functionality. Fortunately, more vendors are including standards-based interfaces to support integrated functionality. We anticipate this industry trend to continue due to customer demand for integrated functionality.

Coordinated management has emerged with the advent of the standards organizations information models. These information models along with the object-oriented modeling permit the representation of the enterprise environment as a single managed system. Elements within the managed system can be associated to reveal and manage working relationships such as workflow and hierarchy dependencies. This abstraction of the human, business and technology relationships is at the core of business rule-based policy enforcement and is a cornerstone of PBNM.

The primary enabling technologies are directory services and XML. Security requirements for strong authentication and authorization in an increasingly hostile world are driving industry adoption of directory services. XML is a sister protocol to the hypertext markup language (HTML) and is part of a subset of the standardized generalized markup language (SGML). The XML standards include a family of markup languages that allow for the transport of information between disparate systems. These developments enable a new paradigm of end-to-end information services supported by the object oriented modeling of directory services, the textual nature of XML-enabled network configuration and a common set of baseline technologies.

The logically managed system described in this report parallels the Burton Group[8] virtual enterprise network (VEN). The Burton Group technology positions and reference architectures include SOA, an enterprise service bus, web services framework and identity and access management (I&AM) among other elements. The TMF SID and DEN-ng involve similar SOA functionality, where a "publish and subscribe" message bus and lookup services, such as JINI/JLS are incorporated for PBNM. The desired functionality section of this report combines these concepts to facilitate enterprise attribute sharing, event correlation and end-to-end service delivery.

[8] www.burtongroup.com

Translating business language to technology terminology requires a level of abstraction in which business entities and relationships (parties, contracts and service level agreements) are represented in kind with systems and network entities (services and resources). The DMTF and TMF have addressed this need with the DEN and CIM, and SID and DEN-ng information models, respectively. These developments parallel and complement the wholesale adoption of directory services by network operating system vendors. Therefore, we observe that the baseline enabling technologies of directory services, XML and distributed application architectures (i.e. J2EE) underpin PBNM, IdM and SOA. This technology symmetry and abstraction capability makes possible the binding of business process and policy to the application, computing, network and operational support system elements of the enterprise network.

The standards organizations and industry alliances provide guidance for the integrated enterprise network. They include the Organization for the Advancement of Structured Information Standards (OASIS)[9], the Liberty Alliance[10], the IETF[11], DMTF and TMF. Pertinent activity is briefly covered here and further information can be found at the respective websites.

The OASIS organization is developing structured information standards in support of eBusiness and web services. OASIS is sponsoring enterprise universal description and discovery integration (UDDI), a registry and lookup service and XML standards. Membership includes BEA Systems; Entrust; Hewlett-Packard; IBM; Intel; Microsoft; Novell; Oracle; Sun Microsystems; Verisign and many more.

The Liberty Alliance is building specifications in support of web authentication. Its mission is to establish an open standard for federated network identity through open technical specifications. Membership includes Entrust, RSA security, Sun Microsystems, Novell, Verisign and many others.

The IEFT originated the X.500 directory access protocol (DAP) and LDAP standards in 1988. Since that time related technologies continued to develop. Relevant RFCs include the IETF Network Working Group's RFC 2768, Network Policy and Services: A Report of a Workshop on Middleware, February 2000 and the February 2004 RFC 3703 Policy Core Lightweight Directory Access Protocol (LDAP) Schema (PCLS). RFC 3703. This work addresses the development of the PCLS and a Policy Core Information Model (PCIM). In addition, the IP Security Policy (IPSP) working group is working to define a common set of terms used in documents in the area of PBNM.

The DMTF has announced the release of CIM Schema 2.9.0. CIM provides a common definition of management information and offers modeling for distributed information architectures, such as Java™ 2 Enterprise Edition (J2EE) environment. This version of CIM facilitates management profiles, management of security principals and authentication policy. CIM and DEN where the result of early Microsoft and Cisco collaboration.

The TMF offers the directory-enabled networks new generation (DEN-ng) and shared information data model (SID). The TMF DEN-ng information model defines policy models to accommodate different domains. For example, the service model defines customer-facing services and resource-

[9] http://www.oasis-open.org/home/index.php

[10] http://www.projectliberty.org/

[11] http://www.ietf.org/rfc/rfc2768.txt

facing services and the resource model defines logical and physical recourses. DEN-ng building blocks include an information model, policy language and a data dictionary. The TMF SID comprises a set of object-oriented information and data models that logically represent entities in managed network environments. The SID and DEN-ng models describe business, system, implementation and runtime policies, processes and data, which are defined using UML class models and the object constraint language (OCL).

The TMF has developed the new-generation operations systems and software (NGOSS) architecture. NGOSS offers the definition of lifecycle process, architecture, methodology that provides a framework for the definition, design and development of integrated operational support systems such as CEM. NGOSS, Release 4.5 has been expanded to include the Service Framework guide book. The TMF provides comprehensive information models and an enhanced Telecom Operations Map (eTOM) business process framework to support NGOSS.

The TMF information models offer methods of managing the state of elements within the PBNM system, expressed in the form of a finite state machine that permits pre-condition, current condition and desired or post condition state to be managed. The finite state machine is essential to the audit, verification and roll back functional requirements of PBNM.

The Intelliden R-Series software suite is closely aligned with the TMF NGOSS, SID and DEN-ng standards. The Colorado Springs-based company had developed the R-Series application in stealth for two years before announcing product availability in early 2002. At the time of this writing, Intelliden offers the only commercially available directory-enabled, TMF compatible multi-vendor network-device management application.

Intelliden R-Series deployments are occurring in the some of the world's largest networks. These include British Telecom and Boeing Corporation. Boeing has licensed the Intelliden R-Series product for the Next Generation Intranet and Secure Mobile Architecture efforts. Boeing is using Intelliden in the "Secure Mobile Architecture" to demonstrate the management of the mobile components in an enterprise environment. PBNM is also having an impact in the wireless arena. One example is the Boeing and Cisco Mobile and Directory (MaD) project. MaD is investigating the feasibility of automated wireless network deployment for airports. In addition, The Royal Nederland's Army (RNLA), NATO and the United States Defense Department have licensed Intelliden R-Series software.

AT&T has claimed to have the largest IP network in the world. In September 2003 AT&T announced the investment and adoption of application aware networks. This investment will install an IP voice-based carrier infrastructure. AT&T will realize a cost savings by moving to VoIP and multi-protocol label switching (MPLS) bypassing regional Bell holding company (RBHC) access charges. Application aware networks employ a two-layer network engine, where the physical (Phy) network provides connectivity services and the logical network provides application and mediation services. This architecture allows managed services and global connectivity services as AT&T transforms from a telephony company to a data company. Information from the 2003 Burton Group Catalyst conference revealed that directory-enabled network services and XML are integral components of AT&T's application aware networks architecture.

These product reviews are brief and do not represent an exhaustive evaluation. Product capability comments pertain to each specific product and no attempt has been made to evaluate these products against a common set of criteria. The intention is to present industry activity and direction with regard to policy management systems. These product reviews were conducted by analysis of technical white papers, product data sheets, vendor and consultant teleconferences, and live demonstrations.

Company information: Intelliden Corporation

http://www.intelliden.com

Intelliden R-Series Software Suite Product capability:

The Intelliden R-Series Software suite (version 4.1) is the only network management product we found that uses a directory service as a core policy repository. Intelliden provides Cisco, Nortel, Foundry and Nokia product support. The product architecture is extensible to multi-vendor support based on TMF SID and DEN-ng standard compatibility. A standards-based SOAP and Java application-programming interface is provided. Core competencies include configuration management, security management, auditing and reporting, provisioning and activation.

Method of review

Live demonstration and discussion, review of technical white papers prepared by the vendor, and dialog with the Burton Group.

Comments

We see the use of a directory service as the core policy repository as an advantage for several reasons. First is the information model that a directory service supports. The information model permits logical representation and object oriented design where individual elements of the managed system are modeled and associated as part of the whole. This allows users to be associated with resources and policies. Second, integration with other directories and repositories is enhanced through the use of the LDAP and XML protocols. Further evaluation is needed to assess full capability and alignment with Sandia criteria. Alignment with the TMF SID and DEN-ng standards is seen as a strong advantage. In addition, Intelliden has developed integration with many of Sandia's selected CEM vendors. These include IBM, Cisco, Visionael, Hewlett-Packard and MicroMuse.

Company information: Enterasys Networks

http://www.enterasys.com/home.html

Enterasys User Personalized Network and NetSight Atlas Policy Manager Product capability

Enterasys has a lead in policy-based networking with their early delivery of user-centric policy-based network and security management called "User Personalized Network" architecture. The NetSight Atlas Policy Manager follows a two-tier architecture in which the policy decision point and policy enforcement point are collocated via agent software on the network device. The user-personalized network technology is proprietary and supports role-based administration. RADIUS, 802.1X and media-access control (MAC) authentication are also supported. Enterasys has stated the intention to develop directory-enabled network capability.

Method of review

Burton Group Research Report: The User Personalized Network: Enterasys' Policy-Based Management v2, May29, 2003, product data sheets and Enterasys Marketing discussion.

Comments

Further evaluation is needed to assess full capability and alignment with Sandia criteria.

Company information: Cisco Systems

http://www.cisco.com/

Cisco CiscoWorks Product capability

Cisco offers an integrated suite of CiscoWorks management tools. CiscoWorks includes the QoS Policy Manager, LAN Management Solution, Small Network Management Solution, Routed WAN Management Solution, IP Telephony Environment Monitor, Voice Manager and the VPN/Security Management Solution.

Method of review

Vendor interview and technical white papers

Comments

These solutions offer a comprehensive tool suite for Management of the Cisco networked environment. Further evaluation is needed to assess full capability and alignment with Sandia criteria. CiscoWorks is an active component of the network management strategy, but is not fully utilized.

Cisco IP Solutions Center Security Policy Manager Product capability

Cisco offers the IP Solutions Center Security Policy Manager as a component of the IP Solutions Center Security Management suite. The IP Solutions Center Security Policy Manager is targeted at VPN, NAT and QoS Cisco technologies. These solutions offer RBAC for the Cisco networked environment.

Method of review

Vendor web site and technical white papers

Comments

Although Cisco is involved with the MaD project and DEN was invented by John Strassner while at Cisco, policy products are designed for proprietary policy domain architecture. Cisco has recently announced upgrades to the integrated security systems, which include the notion of self-defending networks and Cisco Security Agent. Cisco has recently sponsored the industry Network Access Control initiative. Further evaluation is needed to assess full capability and alignment with Sandia criteria.

Cisco Identity Based Network Services Product capability

Identity based network services offers switch port authentication using the 802.1x protocol suite. A workstation is allowed port access restricted to a RADIUS or TACACS authentication server. Once authenticated the port is enabled for network access. The RADIUS or TACACS server can be integrated with an LDAP server for authentication.

Method of review

Vendor interview and technical white papers

Comments

Identity based network services may be of interest in a more comprehensive security solution and prove to be compatible with PBNM as an additional authentication and access-control method. Further evaluation is needed to assess full capability and alignment with Sandia criteria.

Findings

The proliferation of directory service technologies and industry adoption of XML is evident. The genesis of the PBNM proof-of-concept effort was interest in how these new technologies could be used to better manage the Sandia enterprise network. The proof-of-concept PBNM evaluation yielded positive results with the binding of identity with policy as the primary mechanism for enforcing network access-control. The software versions used for the proof-of-concept were Cisco IOS 12.1(13) and Cat OS 6.2(2). The evaluation was conducted using Intelliden R-Series software 3.0 and Cisco 6500 series network equipment. The test plan for the proof-of-concept can be viewed with the following Sandia Web FileShare document link.

HTTPS://wfsprod01.sandia.gov/groups/srn-uscitizens/documents/document/wfs088335.pdf

The DMTF and TMF information models were of particular interest in that the application of these technologies made possible automated control of the network. Historically, (the 1990's) this class of technology was, and remains the base for systems and application management systems such as IdM. More recently, these technologies are being applied to network management systems such as PBNM. This presents an interesting proposition: the alignment of network and systems architecture to enable end-to-end management of network services.

The team has identified significant activity in the industry to support a PBNM capability. During this exercise, two things became clear. First, the baseline technologies enabling automation of network services and information management are prevalent in the industry. Second, industry standards collectively support a new paradigm of end-to-end service delivery.

The state of the art technologies that enable the application of business rules to the management of network device configuration are rooted in the IETF, DMTF and TMF industry standards. Pertinent development goes back to 1988 with the ratification of the IETF X.500 standards. Directory services deployment has experienced recent resurgence due to the need for distributed communication and security. Directory services help to address these needs by providing an object-oriented architecture, which permits the association of human and business elements with network resources.

Automated configuration/change management is the key to rule-based policy enforcement, without which policy enforcement is a tedious manual process, at best targeted at partial functionality. The benefits of automated configuration/change management include increased value and availability of network services, whereby human error is reduced and consistency in configuration is increased. In addition, automated configuration/change management can be leveraged to enforce specific actions based on predefined response to specific threat or condition.

The highest impact is increased cyber security. A hardened security posture is attainable through automated configuration/change management. Network device configuration is commonly performed manually and network protection mechanisms are typically address based. Address-based protection mechanisms remain in use, but with PBNM, cyber security is strengthened with more robust technology. The notion of identity attributes that are associated with rule-based policy is a significant innovation. In addition to identity-based policy enforcement, a network quarantine model was developed where PBNM configuration/change management is used to manage virtual local area network (VLAN) and TCP/IP subnet addresses parameters on switch port and router interfaces. PBNM configuration control can be used to manage these parameters dynamically to support security

processes (i.e. scanning and remediation) by providing an event correlation capability for triggering configuration changes. This model is also compatible with technologies such as 802.1X.

We have tracked the state of the industry and arrived at the purpose of using identity and policy information as a means for cyber-enterprise control. The identity-based policy enforcement case presented in this report brings identity attributes and policy enforcement to bear with the delivery of end-to-end information services.

The development of coordinated PBNM, IdM and SOA capabilities is a daunting challenge. One caveat is that participation and consensus from the various enterprise-management authorities is required and that established barriers are torn down for collaborative pursuit. An audit of existing policy will be necessary to quantify and categorize cyber policy that can be implemented in the PBNM system. Furthermore, consistent semantics need to be adopted for success in this effort. In addition to common policy expression for consistent policy-rule execution, common-naming conventions are needed to ease communication between elements within the enterprise system.

PBNM delivers a standards-based solution and demonstrated interoperability with elements of the enterprise network and supporting technologies. We believe that PBNM, IdM and SOA will provide a framework to support strategic objectives and goals. These include championing the development of effective and robust processes that integrate work across all processes within the ISO 9001/2000 framework, increasing the value of service to customers and improvement of Sandia's information deliver service capabilities. PBNM will help to address operational gaps in achieving automation and the challenge of managing a multivendor network systems environment. The effort will result in the development of embedded processes that advance performance excellence and process improvement.

Sandia is making progress toward this end in many ways with the efforts of various technology teams. CEM leads the way toward an end-to-end management structure, while EDS and IdM are approaching account and entitlement provisioning. PBNM complements these efforts with a workflow engine and XML-enabled configuration management to achieve automation and provisioning that is tightly controlled and based on standard technologies.

[This Page Intentionally Left Blank]

CONCLUSION

The decision to deploy PBNM is pertinent to meeting four Sandia operational challenges. The first is from a daily operations standpoint. Sandia is facing an increasing attrition rate of support staff that will impact network operations significantly in the next few years. Many of the network operations staff are or are soon to be eligible for retirement, while others have been reassigned or moved on to new tasks. The impact on daily operations is high, affecting the management, project lead and staff ladders. Secondly, the attrition trend coincides with increased demands on the network infrastructure. We are simply asked to do more with less, as support resources are limited (and getting more so). These two factors are driving the need for an automated configuration/change management capability to alleviate operational constraints. Process-controlled network device configuration benefits include a reduction of human error, increased consistency of deployment and faster trouble-response time.

The third operational challenge involves CEM functionality. The PBNM automated configuration/change management capability is tightly coupled with the CEM configuration component of the SFCAP model. The PBNM system will interconnect with MicroMuse, Visionael, HP OpenView and other CEM systems. The Intelliden R-Series software suite is directory service and XML enabled. Standard-based interfaces are used for communication with the other elements of the enterprise network. In this context PBNM is central to integrated communications. PBNM facilitates integrated communication for application, computing, network and operational support systems. Automation is further facilitated with the use of an enterprise service bus for attribute sharing and event correlation.

The fourth operational challenge is cyber-security. The baseline technologies that enable automation are embedded in the operating systems and network equipment that we purchase today. We must manage these sophisticated capabilities or risk opening our environment to new vulnerability. Configuration and change management are critical to a well-managed network and therefore cyber-security. PBNM addresses this need with process-controlled workflow and predefined policy. Predefined policy is also useful for automated response to emergency situations or threat. In addition, the use of identity attributes (identity and role of the user and device) for control of physical network protection mechanisms further promotes security.

The SOA approach presented in this report incorporates an enterprise service bus for both systems and network services architecture. Such an approach would facilitate coordinated account, entitlement and network service provisioning with the combined use of PBNM, IdM and SOA.

Policy management must first be considered from a business perspective. Policy definition begins with an understanding of why we do business, the way we go about accomplishing our mission and with whom we do business. Industry standards provide the framework to relate business to technology so that business rules can be used to drive service delivery. This layer of abstraction constitutes a control plane where both user purpose and device functionality utilize role-based definitions. Device programming is accomplished through standard methods, which include SNMP, CLI and XML. In this way, customer facing service and resource facing services can be defined and managed for end-to-end information service delivery.

We conclude that PBNM is a viable solution that meets the information management needs of Sandia and its customers. PBNM is based on state of the art technologies, but rooted in established standards and available (off the shelf) technologies.

Develop A Policy Based Network Management Implementation Plan

The proof-of-concept technical evaluation is complete and indicates that a standards-based PBNM implementation is feasible. A pilot implementation is the recommended next phase, followed by broader deployment as appropriate requirements are identified. The PBNM solution will be supplemented by business-specific policy and process. The PBNM system will integrate with CEM tools and the enterprise environment. Requirements include enterprise directory service authentication, an automated workflow, configuration change management and integration with operational systems and software tools.

Develop An Automated Network Device Configuration/Change Management Capability

Automated network configuration/change management provides a means for managing the complexity of current and future network needs. We recommend the use of the Intelliden R-Series product because of its core capabilities; configuration management; security management; auditing and reporting; activation and provisioning.

Develop A PBNM Security Filter Implementation Plan

A security filter capability would enable the association and use of security policy with automated network device management as a means to rapidly respond to emergency situations. Predefined security filters supplemented by security-specific policy and process would support a hardened cyber-security stance. The proposed PBNM security filter capability will be developed as part of an enterprise defense-in-depth strategy to facilitate coordinated firewall configuration, network quarantine and threat mitigation.

Develop An Enterprise Service Bus And Identify End-To-End Service Opportunities

Information resides in data repositories and must be secure yet accessible. Secure accessibility is dependent on the technologies that permit information exchange. These technologies include the XML standards, SOAP, Java, J2EE, JNDI, JINI, LDAP and others. The resulting implementation could be deployed as an enterprise service bus to facilitate event correlation, service registration, and attribute sharing within the managed system. Integration efforts must be across organizational boundaries and the participation of information owners (finance, human resources and the line) is required to define the needs of the customer and identify end-to-end service opportunities from a business standpoint.

Develop Specific Business, System And Implementation Specifications Using The TMF Information Models

The TMF SID provides a framework to model business, system and implementation viewpoints detailing all *managed elements* within the managed system. Business-specific terms appropriate to the SID should be developed so that business process can be used to drive network configuration. DEN-ng provides a framework to model business, system and implementation viewpoints detailing *network elements and services*. Network service-specific terms appropriate to DEN-ng should be developed for enhanced network service provisioning.

Develop An Enterprise Policy Specification

An enterprise policy specification with participation from the various enterprise-management authorities is a requirement for deploying an end-to-end architecture for large multi-site networks. The enterprise policy specification comprises security policy utilized for access-control, detection, alarm and notification; quality of service (QoS) policy utilized for network traffic management and policing; and operational policy utilized for workflow, approval and process control. The Ponder policy language, the TMF SID and DEN-ng information models, the policy continuum and XML provide a functional model for this work.

Develop An Integrated Enterprise Directory Service

A holistic approach is needed to address the complexity of the enterprise network environment. Work should proceed from a vendor neutral stance and strive to service the diverse multi-platform computing and network enterprise environment with standards compliant technologies. In addition to the variety of operating system and network vendors, integration with various data repositories is fundamental to enable account, entitlement and network service provisioning. All too often network and computing initiatives are developed separately, which in effect disables the continuity needed for a comprehensive enterprise service capability. Development should proceed with network and computing functions considered as a complete system to support end-to-end service delivery.

Develop Identity-Based Policy Enforcement

Policy and identity management are inseparable. Standard interfaces and an enterprise service bus that facilitates attribute sharing and event correlation would serve to integrate PBNM and IdM. This makes possible the association of identity information and network device policy enforcement. Identity-based policy enforcement is based on the premise that PBNM and IdM are integral.

Establish An Enterprise Information Services Architecture

Establish an enterprise information services architecture to accommodate the identification and quantification of corporate information services. The notion of customer-facing services and resource-facing services provides a baseline for the information services architecture. Information services architecture should bridge systems and network architectures for coordinated service delivery.

Ensure PBNM Network Architecture Conformance

Establish a network architecture compliant PBNM capability as a means to increase network availability through consistency in configuration and reduction of human error. PBNM will enhance the maintenance and management of network architecture interface specifications and delivery of to-be-built- network services. The TMF information models serve as a means to normalize network service capabilities so that consistency of service can be maintained across disparate technologies.

Future PBNM Development Path

A future PBNM development path could include Cisco network devices and baseline CEM integration (FY05), Foundry network devices, ISO 9001/2000 process improvement (FY06), Aruba wireless network devices, security policy enforcement (FY07), enterprise systems integration, IdM integration (FY08), network services definition, provisioning and activation (FY09), SOA support (FY10).

Further recommendations will be developed as the PBNM project progresses.

REFERENCES

Published Material:

Understanding Policy-Based Networking
By Dave Kosiur
Wiley Computer Publishing
Copyright © 2001

Directory Enabled Networks
By John Strassner
Macmillan Technical Publishing
Copyright © 1999

Policy-Based Network Management
Solutions For The Next Generation
By John Strassner
Morgan Kaufmann Publishers
Copyright © 2004

Burton Group Research & Technology reports
Network and Telecom Strategies

- Securing the Virtual Enterprise Network: V2, May23, 2003, Analyst Daniel Blum
- "Whatever Happened to Policy-based Networking?" v. 21 Oct 2002, Analyst: David Kosiur
- "Developing Identity Management and Directory Services Architecture Principles, Technical Positions, and Templates," v. 1 November 8, 2002, Analysts: Randall Gamby and Daniel Blum
- "Liberty Alliance: Federated Identity Standards Gain Acceptance," v. 1, March 11, 2003, Analyst: James Kobielus

DEFINITION OF ACRONYMS

ACL - Access-Control List
CEM - Cyber Enterprise Management (Sandia Specific)
CIM - Common Information Model
CLI - Command Line Interface
COPS - Common Open Policy Service
CoS - Class of Service
DEN - Directory Enabled Networks
DEN-ng - Directory-Enabled Networking new-generation
DHCP - Dynamic Host Configuration Protocol
DiffServ - Differentiated Services
DMTF - Distributed Management Task Force
DNS - Domain Name Service
DTD - Document Definition Types
eTOM - enhanced Telecom Operations Map
FCAPS - Fault, Configuration, Auditing, Performance and Security
HTML - Hypertext Markup Language
I&AM - Identity and Access Management
IBNS - Identity Based Network Services
IdM - Identity Management
IntServ - Integrated Services
J2EE - Java™ 2 Enterprise Edition
LDAP - Lightweight Directory Access Protocol
MAC - Media-Access Control
MaD - Boeing and Cisco Mobile and Directory Project
MIB - Management Information Base
MPLS - Multi-Protocol Label Switching
NATO - North Atlantic Treaty Organization
NGOSS - New Generation Operations Systems And Software
OASIS - Organization for the Advancement of Structured Information Standards
OCL - Object Constraint Language
PBNM - Policy-Based Network Management
PCLS - Policy Core Lightweight Directory Access Protocol Schema
PDP - Policy Decision Point
PEP - Policy Enforcement Point
PKI - Public Key Infrastructure
QoS - Quality of Service
RBAC - Role-Based Access Control
RBHC - Regional Bell Holding Company
RNLA - Royal Nederland's Army
SFCAP - Security, Fault, Configuration, Auditing and Performance (Sandia Specific)
SGML - Standardized Generalized Markup Language
SID - Shared Information/Data Definitions and Models
SITE - Sandia Integrated Test Environment (Sandia Specific)
SOA - Service Oriented Architecture
SOAP - Simple Object Access Protocol
TCP/IP - Transmission Control Protocol/Internet Protocol
TMF - TeleManagement Forum
ToS - Type of Service
UDDI - Universal Description And Discovery Integration
UML - Universal Modeling Language
VEN - Virtual Enterprise Network
VLAN - Virtual Local Area Network
VOIP - Voice over IP
VPN - Virtual Private Networks
WBEM - Web Based Enterprise Management
XML - Extensible Markup Language
XSD - XML Schema Definition

DISTRIBUTION

1 MS0630 M. J. Murphy, 09600
1 MS9004 R. H. Stulen, 8100
1 MS9151 K. E. Washington, 8900
1 MS0661 G. E. Rivord, 09510
1 MS0806 J. A. Larson, 09330
1 MS0622 D. S. Rarick, 09310
1 MS0823 J. D. Zepper, 09320
1 MS0805 G. L. Esch, 09520
1 MS0630 D. H. Schroeder, 9620
1 MS0453 M.R. Sjulin, 02120
1 MS1094 R. L. Hartley, 03133
1 MS0780 B. C. Whittet, 04138
1 MS1137 B. J. Tejani, 05511
1 MS0784 J. M. Clem, 05512
1 MS0670 L. L. Widler, 05525
1 MS0806 R.R. Olsberg, 05616
1 MS0806 L.G. Pierson, 05616
1 MS0806 J. D. Tang, 05622
1 MS0806 T. D. Tarman, 05622
1 MS1361 D. F. Beck, 06923
1 MS1137 P. C. Moore, 06224
1 MS9012 R. D. Gay, 08949
1 MS9011 B. V. Hess, 08941
1 MS9012 B. A. Maxwell, 08949
1 MS0924 A. B. Harper, 09524
1 MS9019 P.L. Asprey, 089451
1 MS9915 H. Y. Chen, 08961
1 MS0813 R. M. Cahoon, 09311
1 MS0805 G. K. Rogers, 09312
1 MS0806 J.H. Dexter, 09312
1 MS0806 T. L. MacAlpine, 09312
1 MS0806 C. D. Brown, 09312
1 MS0806 D. A. Hansknecht 09312
1 MS0806 G. D. Machin, 09312
1 MS0806 J P. Abbott, 09312
1 MS0806 P. C. Jones, 09317
1 MS0795 A. A. Quintana, 09317
1 MS0795 R. A. Suppona, 09317
1 MS0795 J. L. Taylor, 09317
1 MS0795 P. D. Warner, 09317
1 MS0795 J. G. Heller, 09317
1 MS0139 C. S. Leishman, 09324
1 MS0823 G. E. McGirt, 09324
1 MS0823 D. J. Bragg, 09324
1 MS0823 J. A. Lewis, 09324
1 MS0822 C. Pavlakos, 09326
1 MS0807 J. P. Noe, 09328
1 MS0807 B. J. Jennings, 09328
1 MS0807 S. R. McRee, 09328
1 MS0805 W. D. Swartz, 09329
1 MS0805 M. A. Cinense, 09329
1 MS0805 J. W. Crenshaw, 09329
1 MS0805 M. A. Stilwell, 09329
1 MS0805 T. C. Hobson, 09329
1 MS0805 J. M. Muntz, 09329
1 MS0805 M. W. Gutscher, 09329
1 MS0805 P. S. Kuhlman, 09329
1 MS0805 D. J. Leong, 09329
1 MS0799 G. E. Connor, 09333
1 MS0799 M. J. Ernest, 09333
1 MS0799 J. M. Diehl, 09333
1 MS0799 J. A. Chavez, 09333
1 MS0799 T. Bruner, 09333
1 MS0799 D. Eichert, 09333
1 MS0813 C. A. Morgan, 09333
1 MS0788 M. J. Benson, 09334
1 MS0812 M. D. Gomez, 09334
1 MS0806 L. G. Martinez, 09334
1 MS0806 L. F. Tolendino, 09334
1 MS0788 M. A. Rios, 09334
1 MS0788 V. K. Williams, 09334
1 MS0788 D. W. King, 09334
1 MS0788 D. R. Garcia, 09334
1 MS0806 L. G. Martinez, 09334
1 MS0788 S. D. Olsen, 09334
1 MS0788 G. Rivera, 09334
1 MS0788 T. J. Spears, 09334
1 MS0806 L. Stans, 09336
1 MS0806 J. P. Brenkosh, 09336
1 MS0806 J. M. Eldridge, 09336
1 MS0806 A. Ganti, 09336
1 MS0806 J. H. Naegle, 09336
1 MS0806 S. A. Gossage, 09336
1 MS0806 J. A. Schutt, 09336
10 MS0788 C. M. Keliiaa, 09336
1 MS0806 D. J. Wiener, 09336
1 MS0806 J. S. Wertz, 09336
1 MS0806 B. R. Kellog, 09336

1 MS0806 M. M. Miller, 09336
1 MS0806 E. L. Witzke, 09336
1 MS0788 P. L. Manke, 09338
1 MS0788 E. J. Klaus, 09338
1 MS0788 R. L. Adams, 09338
1 MS0788 R. L. Moody, 09338
1 MS0806 T. C. Hu, 09338
1 MS0806 T. J. Pratt, 09338
1 MS0661 J. R. K. Smith, 09512
1 MS0661 J. R. Schofield, 09514
1 MS0660 D. S. Cuyler, 09514
1 MS0660 A. H. Treadway, 09514
1 MS0660 D. S. Cuyler, 09519
1 MS0660 K. A. Byle, 09519
1 MS0660 K. M. Denton-Hill, 09519
1 MS0920 L, R. Arellano, 09519
1 MS0629 J. A. Fillinger, 09521
1 MS0807 K. E. Wiegandt, 09610
1 MS0899 M E. Adams, 09616
1 MS0807 J. F. Mareda, 09617
1 MS0662 M. D. Snitchler, 09617
1 MS0662 J. C. Kelly, 09617
1 MS0662 C. A. Quintana, 09617
1 MS0662 G. H. Simon, 09617
1 MS0601 P. D. Tejada, 09617
1 MS0805 W. R. Mertens, 09618
1 MS0805 L. R. Garcia, 09618
1 MS0805 A. J. Ambabo, 09618
1 MS0662 R. E. Evanoff, 09622
1 MS0662 J. R. House, 09622
1 MS0662 S. J. Sanchez, 09622
1 MS0924 G. J. Giese, 09524
1 MS0612 A. Van Arsdall, 96122
1 MS9018 Central Technical Files, 8945-1
2 MS0899 Technical Library, 9616