Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Policy-based Network Management System

Demonstration Report

J. Spagnolo and D. Cayer

Defence R&D Canada – Ottawa
CONTRACT REPORT
DRDC Ottawa CR 2006-117
June 2006

Canada

Policy-based Network Management System

Demonstration Report

J. Spagnolo, D. Cayer
NRNS Incorporated

Prepared by:

NRNS Incorporated
4043 Carling Avenue, Suite 106
Ottawa, ON K2K 2A3

Project Manager: J. Spagnolo
Contract number: W7714-3-800/001/SV
Contract Scientific Authority: Dr. S. Zeber, DRDC Ottawa, (613) 991-1388
Contract Scientific Advisor: Mr. T. Symchych, CRC (613) 949-3070

Defence R&D Canada – Ottawa

Contract Report
DRDC Ottawa CR 2006-117
June 2006

The work described in this report was sponsored jointly by the Department of National Defence under the work unit 15BQ and by the Communications Research Centre Canada (CRC) under the work unit 15CS.

Abstract

In April 2006 the PBNM prototype system developed by Defence R&D Canada (DRDC) Ottawa in collaboration with the Communications Research Centre (CRC) was demonstrated to The Technical Cooperation Program (TTCP) Panel 11 using five Administrative Domains (ADs) interconnected by the DREnet as a Wide Area Network (WAN). The purpose of the demonstration was to illustrate how the prototype system automates the configuration and administration of Policy Enforcement Point (PEP) devices using low level policies generated from negotiated high level policies by a Policy Decision Point (PDP). Lessons learned from the demonstration related to the complexity of the policy specification and the non-intuitive nature of the policy administration tool, as well as to the lack of integrity provided by the Policy Repository for policy documents and policy negotiation objects. Further design and development efforts are required to address the deficiencies and issues identified during the planning, implementation, and presentation of the demonstration.

Resumé

Le prototype du système PBNM a été développé par R & D pour la défense Canada (RDDC) - Ottawa, en collaboration avec le Centre de recherches sur les communications Canada (CRC). En avril 2006, on a fait la démonstration de ce prototype pour les membres du Programme de coopération technique (TTCP), volet 11, en se servant de cinq domaines administratifs (ADs) interconnectés par le DREnet de façon à former un réseau étendu (WAN). La démonstration visait à illustrer la façon dont le système prototype automatise les processus de configuration et d'administration de dispositifs associés à un point d'application de politique (PEP), à l'aide de politiques spécifiques établies depuis des politiques générales, par un point de décision de politique. Les conclusions tirées de la démonstration sont liées à la complexité de la spécification de politique, au caractère non intuitif de l'outil de gestion des politiques, et au fait que le référentiel des politiques ne peut assurer complètement l'intégrité des documents sur les politiques et des objets de négociation des politiques. Il faut poursuivre le travail de conception et de développement pour corriger les lacunes et les problèmes relevés pendant la planification, la mise en œuvre et la présentation de la démonstration

This page intentionally left blank.

Executive summary

Policy-based Network Management System: Demonstration Report

Spagnolo, J., Cayer, D.; DRDC Ottawa CR 2006-117; Defence R&D Canada – Ottawa; June 2006. [D7]

Introduction

In April 2006 the Policy Based Network Management (PBNM) prototype system was demonstrated to The Technical Cooperation Program (TTCP) Panel 11. The demonstration, which involved five administrative domains (ADs) connected over the DREnet as a wide area network (WAN) was given at the DRDC Ottawa site. The purpose of the demonstration was to illustrate the policy negotiation capability of the PBNM prototype system, as well to highlight some of the more advanced features of the prototype system.

Results

The planning, implementation, and delivery of the demonstration exposed deficiencies in the system and also revealed several issues that require further investigation. Some of the deficiencies and issues can be addressed with minimal or moderate design and development effort while others require significant design and development effort. The main lessons were related to the complexity of the policy specification and the non-intuitive nature of the tool supplied to edit the policy, as well as to the lack of integrity provided by the Policy Repository for policy documents and policy negotiation objects.

Significance

The TTCP Panel 11 meeting provided the first opportunity to demonstrate the PBNM prototype system to organizations other than Defence R&D Canada (DRDC) and the Communication Research Centre (CRC). The participants provided valuable comments on the potential use of PBNM technology within military environments.

Future plans

A short-term investigative task should be undertaken to examine the technologies and approaches for addressing the identified deficiencies and issues. The investigation should produce a longer term plan that identifies suitable technologies and approaches and provides estimates for the level of effort required to implement the plan

Sommaire

Policy-based Network Management System: Demonstration Report

Spagnolo, J., Cayer, D.; DRDC Ottawa CR 2006-117; R & D pour la défense Canada – Ottawa; juin 2006. [D8]

Introduction

En avril 2006, on a fait la démonstration du prototype du système de gestion de réseau basée sur des politiques (PBNM) à l'intention des membres du Programme de coopération technique (TTCP), volet 11. La démonstration s'est déroulée au site RDDC Ottawa. Elle mettait en cause cinq domaines administratifs (AD) interconnectés par le DREnet de façon à former un réseau étendu (WAN). Elle visait à illustrer la capacité de négociation de politiques du système prototype PBNM ainsi que certaines des fonctions évoluées du système.

Résultats

Lors de la planification, de la mise en œuvre et de la présentation de la démonstration, on a relevé un certain nombre de lacunes dans le système ainsi que plusieurs problèmes qui doivent être examinés. Dans certains cas, des efforts minimes ou modérés de conception et de développement suffiront pour trouver une solution. La résolution de certains autres problèmes demandera toutefois beaucoup plus de travail. Les conclusions tirées de la démonstration sont essentiellement liées à la complexité de la spécification de politique, au caractère non intuitif de l'outil d'édition des politiques fourni, et au fait que le référentiel des politiques ne peut assurer complètement l'intégrité des documents sur les politiques et des objets de négociation des politiques.

Signification

La rencontre avec les membres du TTCP, volet 11, a permis de faire la première démonstration du prototype du système PBNM pour une organisation autre que R & D pour la défense Canada (RDDC) et le Centre de recherches sur les communications Canada (CRC). Les participants ont fait des observations très utiles sur l'utilisation possible de la technologie PBNM dans les environnements militaires.

Perspectives

Il faut entreprendre à court terme l'examen des technologies et des approches qui permettraient d'apporter une solution aux lacunes et aux problèmes relevés. Cet examen donnera lieu à l'établissement d'un plan à plus long terme dans lequel on identifiera les technologies et les approches qu'il y a lieu d'appliquer et on indiquera le niveau d'effort requis pour procéder à la mise en œuvre du plan.

Table of contents

This page intentionally left blank.

1. Introduction

Defence R&D Canada (DRDC) Ottawa and the Communication Research Centre (CRC) have collaborated to develop a prototype Policy Based Network Management (PBNM) system that provides an automated means to configure and administer Policy Enforcement Point (PEP) devices such as virtual private network (VPN) gateways, firewalls and routers using lower level PEP-specific policies generated from high level policies by a Policy Decision Point (PDP).

The R&D effort has produced an extensible PBNM system framework [1] that is able to negotiate and implement policies, and a specification for an inter-domain security policy [2] that is currently the only policy type implemented.

2. Purpose

In April 2006 the PBNM prototype system was demonstrated to The Technical Cooperation Program (TTCP) Panel 11. The demonstration involved five Administrative Domains (AD) connected across a Wide Area Network (WAN). Defence R&D Canada (DRDC) Ottawa hosted two ADs, the Communication Research Centre (CRC) hosted two ADs and NRNS Incorporated hosted a single AD. The demonstration was delivered at the DRDC Ottawa site and followed the demonstration plan described in [3]. The purpose of the demonstration was to illustrate the policy negotiation capability of the PBNM system, as well as to highlight some of the more advanced features such as remote restrictions and external events.

This document discusses the issues, deficiencies and lessons learned from planning the demonstration, implementing the demonstration environment, and delivering the demonstration to TTCP Panel 11. This document also identifies future work that will address certain deficiencies and improve the PBNM system.

3. Deficiencies

3.1 Policy Negotiation Cycling

During the demonstration rehearsals as well as the demonstration itself, policy negotiation between certain ADs would cycle through most policy negotiation states but unexpectedly restart at the beginning of the negotiation sequence causing the negotiation to never complete. This problem was attributed to a programming error that has since been resolved. The software was correctly detecting duplicate Policy Proposal objects but was not discarding them.

3.2 Policy Locking

When the Security Officer uses the Policy Editor to connect to the PDP and edit the policy, the PDP locks the policy to prevent concurrent access which may lead to lost policy updates. During the demonstration rehearsals, a local intermittent network outage experienced while editing the policy forced the Security Officer to abandon a Policy Editor session on one workstation and re-establish a Policy Editor session on another workstation. The Security Officer was unable to acquire the policy via the second session since the policy remained locked by the initial session. Although this was the expected and correct behaviour, the PBNM Operator Console contained no indication that the policy remained locked.

The PBNM Operator Console requires an Alert Model for the Policy Submission Point (PSP) that displays the status of all policy documents and, if the policy is locked, includes the digital identity and Internet Protocol (IP) network address of the Security Officer that has locked the policy.

3.3 No Reason Given for Local Confict

Certain demonstration scenarios caused a remote AD to be placed in the Local Conflict state when the local AD could not compile a compliant policy proposal for the remote AD. One of the demonstration observers noted that the PBNM prototype system did not provide any information that described the reason why a compliant proposal could not be created for the remote AD.

The local AD places the remote AD in the Local Conflict state when:

- the address space claimed by the remote AD conflicts with the address space claimed by a higher priority remote AD;
- the domain name space claimed by the remote AD conflicts with the address space claimed by a higher priority remote AD;
- a critical service offered to the remote AD is precluded by the remote service restriction of a higher priority remote AD; or
- the priority of the AD is below the threshold mandated by the current Threat Level.

The PBNM system should store the reason for placing a remote AD in the Local Conflict state and should make the information available via the Operator Console.

4. Lessons Learned

This section presents the key lessons that were learned while planning the demonstration, implementing the demonstration environment, and delivering the demonstration to TTCP Panel 11. Some of these issues were observed by the Contractor, DRDC personnel or CRC personnel, while others were derived from comments and feedback provided by Panel 11 members during and after the demonstration.

4.1 Policy Specification

The Inter-Domain Security Policy presented in [2] describes the policy specification for security policies exchanged and negotiated between different ADs. This policy specification was compiled as a sample policy for the purpose of designing, implementing and testing the PBNM prototype system. The authors of the Inter-Domain Security Policy specification included a level of abstraction with the use of predefined security classes and services in order to create a higher-level policy specification, but still intended that the policy be compiled and maintained by a subject matter expert such as the organization's Security Officer.

The demonstration required that the Contractor compile five separate policy documents – one for each participating site. Although the Contractor authored the Inter-Domain Security Policy specification and possessed experience in compiling policies based on the specification, the Contractor did experience some difficulties in creating the required policies. The difficulties were in part attributed to the complexity of the policy specification, which includes multiple policy scopes that must be aggregated, priorities to resolve conflicts, as well as remote restrictions that cause service offerings to be revoked. The difficulties may also have been attributed and to the non-intuitive operation of the PBNM Policy Editor, which is based on a generic eXtensible Markup Language (XML) based editor.

The Inter-Domain Security Policy specification needs to be examined and altered to support operational environments. Features that serve no operational purpose should be removed.

4.2 Security Class and Service Mapping

The Inter-Domain Security Policy specification includes a level of abstraction with the use of predefined security classes and services. Security classes and services are simply referenced by name within the policy document. These higher-level constructs are resolved after the policy negotiation completes successfully and the PBNM prototype system converts the merged local and remote policy proposals to create a lower-level policy suitable for PEP devices. Currently, the PBNM prototype system must be able to acquire the necessary information associated with these names or the system will encounter an exception and cease operation. The PBNM prototype system should ensure that the names used within the higher-level policy are valid when a Security Officer submits a new policy via the Policy Editor. The PBNM prototype system should ensure that the names included within a policy proposal received from a remote AD are valid immediately upon reception of the policy proposal object. These measures ensure that the PBNM

prototype system reports the error immediately to the source of the erroneous information and that it can later resolve the names to produce the lower-level policy.

Policy proposal objects exchanged as part of the policy negotiation sequence contain the higher-level names for security classes and services. The PBNM system design assumes that these names resolve to the same information on all PDP systems. If the names resolve to different information, the resulting lower-level policies may be inconsistent and may result in dysfunctional PEP device configurations. Alternatively, the PBNM system could include expanded security class and service information within policy negotiation objects. However, this would greatly increase the size of these policy negotiation objects and amplify the network bandwidth requirements.

4.3 Integrity of the Policy Repository

When the PDP starts, it searches the policy repository for the most recent policy document. Although the policy document contains a timestamp attribute within the signed portion of the policy document, the Policy Repository does not base its search on that attribute since the Policy Repository, like the majority of the PBNM software, is policy-independent and considers policy documents and policy objects to be opaque. Instead the Policy Repository bases its search on a timestamp attribute contained within a generic repository wrapper. Since the generic repository wrapper is not protected by a digital signature, the contents of the timestamp attribute can be altered causing an older policy document to be deemed the most recent policy document. Even if the Policy Repository could base its search on a protected timestamp attribute, the system can still be deceived into selecting an older policy as the most recent policy document if the newest policy document was deleted from the repository.

Although the PBNM system digitally signs all policy documents and policy objects before storing them in the Policy Repository, the system is susceptible to tampering. The PBNM Policy Repository must provide complete data integrity for policy documents and policy objects.

4.4 Overhead of Java Serialization

The PBNM prototype system leverages Java serialization to exchange information from one PBNM component to another. This includes information exchanged between the Policy Negotiation Proxy (PNP) system in the local AD and the PNP systems in remote ADs. For the most part, PBNM network communication is achieved using ObjectReaders and ObjectWriters to transmit and receive XML encoded objects maintained within Document Object Model (DOM) trees

The TTCP demonstration provided the first opportunity to test the PBNM system in a WAN environment. The demonstration showed that the policy negotiation sequence required considerable more time to complete when policy negotiation objects were exchanged over a relatively slow WAN communication links instead of an ultra high-speed LAN. Packet traces revealed that a single Policy Proposal object transmitted within a serialized Java object consisted of numerous Transmission Control Protocol (TCP) segments of varying sizes.

The practise of using Java serialization to exchange policy objects stored as DOM trees may not be suitable for low bandwidth WAN environments. Other approaches should to be investigated.

4.5 Availability of Remote Services

The policy documents identify the services the local AD offers to a remote AD as well as the services that the local AD expects from the remote AD. Due to the dynamic nature of PBNM policy negotiation, all, part or none of the services may be available to the local user community at any given point in time. Unfortunately the PBNM system does not announce the availability of remote services to the local user community.

The PBNM system should publish the availability of remote services on a web server that is accessible by the local user community.

4.6 Firewall Rule Ordering

The Policy Enforcement Point Proxy (PEPP) software implemented for the Fortigate-60 firewall device adds and removes permissive firewall encryption rules from the device configuration as required to implement negotiated security policies. Traffic not explicitly permitted by a permissive rule is dropped by the implied "DENY ALL" rule. Although the Fortigate device requires that each firewall rule be assigned number, the rule number does not play a role in ordering the rules. Firewall encryption rules added by the PEPP software are appended to the end of Fortigate firewall rule set.

The Fortigate device must be seeded with a few basic firewall rules that permit access between the various PBNM system components – both within the local and remote ADs. These basic rules do not request encryption and as such do not require the presence of a Virtual Private Network (VPN). These basic rules must describe specific traffic flows in detail such that they do not interfere with the firewall encryption rules added afterwards by the PEPP software.

During the demonstration rehearsals, one of the Fortigate devices was not directing traffic to other PBNM sites through the VPN. This was caused by the presence of a residual firewall rule within the Fortigate device that permitted all outbound traffic with no requirement for encryption. It is imperative that only the basic rules that permit access between the various PBNM system components be configured within the Fortigate device when using the Fortigate as a PEP device for the PBNM system prototype.

4.7 External Events

Currently the PBNM system only accepts changes to external events via the Operator Console. An external event is simply a text-based key that identifies the name of the external event and a text string that contains the value of the external event. The PBNM system should accept external event notifications from other systems such as command and control systems or situational awareness systems such as the Joint Network Defence and Management System (JNDMS). A protocol and interface is needed to facilitate the submission of external events from external systems.

4.8 PEP Device Support

The PBNM system currently includes support for a single PEP device based on the Fortigate-60 firewall/VPN appliance. The lower-level firewall and VPN policies used to configure firewall and VPN devices are relatively generic in order to support different PEP devices supplied by different vendors. Unfortunately the generic lower-level policies to not leverage many of the firewall and VPN devices' advance features such as network address translation and intrusion protection.

5. Future Work

The work conducted on the PBNM prototype began in December 2004. Since then other PBNM related research initiatives have started to emerge. These other PBNM research initiatives should be identified and studied to ensure that the PBNM prototype system is aligned with other PBNM related work in order to facilitate future collaboration, to realize interoperability, as well as to avoid duplication of effort.

Section 3, Deficiencies, and Section 4, Lessons Learned, describe numerous issues that should be addressed to improve the PBNM system. Some require minimal or moderate design and development effort while others require significant design and development effort. The issues that require the most design and development effort include the "Policy Specification" issue discussed in section 4.1 and the "Integrity of the Policy Repository" issue discussed in section 4.3.

In the following subsection, the "Policy Specification" issue is further discussed since it would introduce significant changes to the way in which the prototype PBNM system creates, edits, acquires, processes and stores policy documents and policy negotiation objects. A short-term investigative task should be undertaken to examine the technologies and approaches outlined in the following subsection. The investigation should produce a longer term plan that identifies suitable technologies and approaches and provides estimates for the level of effort required to implement the plan.

5.1 Policy Specification

The Inter-Domain Security Policy specification should be re-examined and a second revision of the specification should be compiled.

The existing policy specification defines three policy scopes designed to support hierarchical policy management with higher-level scopes placing restrictions on lower-level scopes. However, the PBNM prototype system only recognizes a single author for the entire policy and does permit different individuals to edit different scopes within the policy. The PBNM prototype system should instead deal with the policy and business requirements as separate documents. The policy should be compiled by security officers and should identify what is permitted and describe the conditions under which it is to be provided. The business requirements should be expressed by managers or commanders and should specify what is needed to fulfill their mandates. The policy will remain a detailed technical document, but high-level abstraction should be used to express the business requirements. The PBNM prototype system must ensure that the business requirements conform to the policy.

Although AD priorities are necessary to resolve conflicts between different ADs, their use may create policy negotiation deadlocks since priority levels are assigned locally and not coordinated with remote ADs. Moreover, mechanisms such as remote policy controls add a great deal of complexity to the system. These features as well as others contained within the current policy specification should be examined to determine their usefulness in operational environments.

The majority of the current PBNM prototype system was designed to be policy independent. Only the Policy Processing Unit (PPU) component of the system is policy aware and contains logic to validate, process and negotiate policies based on the Inter-Domain Security Policy specification. Moreover, the PPU software is implemented as a set of abstract Java classes that include generic functionality needed to acquire new instances of policies and to negotiate policies. All policy specific processing is provided by the distinct PPU class, which extends the base PPU classes to inherit the required generic capabilities. As a result, only the distinct PPU class needs to be re-designed completely and developed in order to implement the second generation Inter-Domain Security Policy specification.

The following subsections describe some additional issues that should be considered when implementing the second generation the Inter-Domain Security Policy specification.

5.1.1 Data Binding

The PBNM system utilizes XML to compile, transmit, process and store policies. The PBNM system deals with policy data as in-memory XML-encoded objects maintained within domain object module (DOM) trees. This has proven to be very inefficient and the resulting Java code very difficult to understand and maintain.

One example of Java data binding technologies is Java XML Binding (JAXB), which converts XML documents to Java objects and Java objects to XML documents. Many other technologies, some open source, have recently appeared in the hope of providing an elegant and efficient solution to the XML data binding problem. These data binding technologies should be examined to assess their suitability in binding external XML-encoded policies into Java objects, which are easier to process than DOM trees and much more efficient than DOM trees.

5.1.2 Policy Persistence

The current PBNM prototype system relies on the Apache Xindice native XML database as its Policy Repository where the PBNM prototype system stores its policy documents and policy negotiation objects. This technology has proven to have poor performance when executing queries against a heavily populated database. Alternate database technologies should be examined to achieve greater reliability and performance for the Policy Repository. At the same time, Java persistence technology should also be examined to facilitate the storage of policy documents and policy negotiation objects. Typically, persistence technology renders a Java class implemented by a programmer as a persistent-capable class that possesses the knowledge and ability to create a copy of itself to persistent storage such as a database.

5.1.3 Rule Based Processing

The current PBNM prototype system performs policy validation and evaluation in Java software. This software includes several thousand lines of complex Java code, which is very difficult to understand and maintain. Moreover, any modification to the specification requires a modification to the Java code.

Rule based processing permits the creation and execution of high-level rules to perform business logic processing. A business-rule language describes the grammar for the specific knowledge domain while a business–level model describes the vocabulary. The rule engine employs inference to emulate the human capability to arrive at a conclusion by reasoning.

The successful integration of a rule based processing system into an application requires the participation of different people with different skills: a software developer, a business or system analyst, and a business manager. The rule based processing system separates the business rules from the source code, thus providing the ability to alter the application behaviour through user-modifiable rules instead of modifying source code.

In addition to commercial offerings, many open-source rule engine frameworks have been implemented. Rule engine technology should be investigated to determine its suitability for inclusion within the PBNM system.

5.1.4 Visual Editors

Ideally, security officers, business managers and commanders should make use of visual editors to create and edit policies and business requirements. Visual editors provide a highly intuitive means for performing complex operations. Visual editor technology should be examined to assess its suitability for editing policies and business requirements. The assessment should consider how changes to the policy and business requirements specification impact the visual editor implementation. Ideally, the visual editor should be configurable from external data using a declarative programming approach.

6. Conclusions

Certain PBNM prototype system deficiencies outlined in this report should be addressed immediately in order to improve the quality of future demonstrations. They include the following:

- the “Policy Locking” issue described in section 3.2;
- the “No Reason Given for Local Conflict” issue described in section 3.3; and
- the “Availability of Remote Services” issue described in section 4.5.

Furthermore, a technology investigation should be undertaken, in the short term, in order to assess the suitability of certain technologies and concepts that can be used to enhance the PBNM prototype system. The investigation should examine technologies such as rule-based processing, data binding, data persistence, as well as visual editors. The investigation should also examine other PBNM initiatives in order to facilitate future collaboration; to realize interoperability; as well as to avoid duplication of effort.

After the completion of the technology investigation, the inter-domain security policy specification needs to be examined and replaced with a second generation policy that permits the PBNM prototype system to deal with business requirements separately from policy. Once the new policy specification is compiled and the relationship between policy and business requirements is established, a new Policy Processing Unit (PPU) must be designed and developed to implement the new policy specification. The PBNM prototype system must also be redesigned to permit the compilation, management and processing of business requirements, which will form the basis for the policy proposals exchanged and negotiated between administrative domains. Design changes to the system should incorporate suitable technologies identified as part of the initial technology investigation.

In the longer term, issues such as policy repository integrity, Java serialization overhead and the external event interface must be examined in advance of transitioning the PBNM system from a prototype system to an operational system.

References

[1] Spagnolo, J., and Cayer, D., (2006). *Policy-based Network Management System – Part 1: System Design Document*, (DRDC Ottawa CR 2006-123) Defence R&D Canada - Ottawa.

[2] Spagnolo, J., and Cayer, D., (2006). *Policy-based Network Management System – Part 9: Inter-domain Security Policy Specification*, (DRDC Ottawa CR 2006-123) Defence R&D Canada - Ottawa

[3] Spagnolo, J., Cayer, D.,(2006) *Policy Based Network Management System: Demonstration Plan*, DRDC Ottawa CR-2006-102, March 2006

This page intentionally left blank.

List of symbols/abbreviations/acronyms/initialisms

API	Application Programming Interface
AD	Administrative Domain
CRC	Communications Research Center
DOM	Document Object Model
DRDC	Defence R&D Canada
PBNM	Policy Based Network Management
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PNP	Policy Negotiation Proxy
PPU	Policy Processing Unit
PSP	Policy Submission Point
TCP	Transmission Control Protocol
TTCP	The Technical Cooperation Program
VPN	Virtual Private Network
WAN	Wide Area Network
XML	eXtensible Markup Language

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

NRNS Incorporated
4043 Carling Avenue, Suite 106
Ottawa, ON K2K 2A3

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

Unclassified

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C, R or U) in parentheses after the title.)

Policy-based Network Management System: Demonstration Report

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Spagnolo, J., Cayer, D.

5. DATE OF PUBLICATION (Month and year of publication of document.)

June 2006

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

13

6b. NO. OF REFS (Total cited in document.)

3

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

NIO Section, DRDC Ottawa

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

15BQ

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

W7714-3-800/001/SV

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

DRDC Ottawa CR 2006-117

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

(.X) Unlimited distribution
( ) Defence departments and defence contractors; further distribution only as approved
( ) Defence departments and Canadian defence contractors; further distribution only as approved
( ) Government departments and agencies; further distribution only as approved
( ) Defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Full Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

In April 2006 the PBNM prototype system developed by Defence R&D Canada (DRDC) Ottawa in collaboration with the Communications Research Centre (CRC) was demonstrated to The Technical Cooperation Program (TTCP) Panel 11 using five Administrative Domains (ADs) interconnected by the DREnet as a Wide Area Network (WAN). The purpose of the demonstration was to illustrate how the prototype system automates the configuration and administration of Policy Enforcement Point (PEP) devices using low level policies generated from negotiated high level policies by a Policy Decision Point (PDP). Lessons learned from the demonstration related to the complexity of the policy specification and the non-intuitive nature of the policy administration tool, as well as to the lack of integrity provided by the Policy Repository for policy documents and policy negotiation objects. Further design and development efforts are required to address the deficiencies and issues identified during the planning, implementation, and presentation of the demonstration.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

coalition network, demonstration, domain policy, policy-based network management, policy constraint, policy enforcement, policy negotiation, policy submission, policy update

Defence R&D Canada

Canada's leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

www.drdc-rddc.gc.ca