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

Policy Based Network Management: Final Report

J. Spagnolo, D. Cayer

Defence R&D Canada – Ottawa
CONTRACT REPORT
DRDC Ottawa CR 2005-112
September 2005

Canada

Policy Based Network Management: Final Report

J. Spagnolo, D. Cayer
NRNS Incorporated

NRNS Incorporated
4043 Carling Avenue
Ottawa, ON
K2K 2A3

Contract Number: W7714-3-800/001/SV

Contract Scientific Authority: Dr. S. Zeber (613) 991-1388

Contract Scientific Advisor: Mr. Tim Symchych, CRC, (613) 949 - 3070

The work described in this report was sponsored jointly by the Department of National Defence under the work unit 15BF and by the Communications Research Center Canada under the work units 15CS and 15CV.

Defence R&D Canada – Ottawa

Contract Report

DRDC Ottawa CR 2005-112

September 2005

Terms of release: The scientific or technical validity of this Contract Report is entirely the responsibility of the contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada or the Communications Research Centre.

Document Revision History

Version 0.1	31-Mar-2005	Complete DRAFT submitted Scientific Authority for review.
Version 1.0	31-Mar-2005	Incorporated comments from Defence R&D Canada and the Communications Research Centre.
Version 1.0	September 2005	Integration of Task 11 Final Report by the DRDC SA .

Table of Contents

List of Figures

1. Introduction

Policy Based Network Management (PBNM) systems provide an automated means to configure and administer Policy Enforcement Point (PEP) devices such as virtual private network (VPN) gateways, firewalls and routers. The Policy Decision Point (PDP) takes high level policies as input and produces lower level PEP specific policies as output. The PBNM system can process different types of policies. When evaluating policies, the PDP must identify and resolve conflicts within competing policies as well as take into consideration external factors such as the time-of-day and the current threat level.

A PBNM system alleviates the need for network administrators to manually configure numerous network devices in order to implement local policy changes. We also introduce the concept of policy negotiation for inter-domain policies[1] such as inter-domain security policies. Negotiable policies are not complete policy documents and therefore the PDP cannot directly implement them. Instead, the local PDP must exchange policy proposals with a PDP in a remote administrative domain. Policy proposals contain all the negotiation parameters needed by the other party to correctly evaluate the proposed policy against the local policy. A PDP can accept a proposed policy in whole or in part or it can reject the proposed policy. If both parties accept the other party's proposed policy in whole or in part, each party merges the local and remote policy proposals to form a complete policy document that the PDP can implement. The PBNM system automatically reconfigures network devices as required to implement negotiated policies.

2. Purpose

This document presents the final report for work conducted by NRNS Incorporated for Tasks 9, 10 and 11 under contract W7714-030800/001/SV for Defence R&D Canada – Ottawa. Task 9 called for the design and development of a framework for a Policy Decision Point (PDP), while Task 10 requested the design and development of a framework for a Policy Negotiation Point (PNP). It was initially thought that these two systems would be equal in complexity and size. However, much of the functionality initially anticipated to reside within the PNP system was subsequently migrated to the PDP system. Moreover, the PNP system was renamed to the Policy Negotiation Proxy (PNP) – a name that better described its diminished role. Task 11 called for the enhancement of the PBNM System to include a functional Policy Server component that is able to interact with PEP devices through the use of the Common Object Open Policy (COPS) for Provisioning (COPS-PR). Task 11 also required the establishment of a problem reporting and tracking system, the expansion of the development and testing environment, and the development of test scenarios

This document describes the activities undertaken by the NRNS Incorporated development team to complete the aforementioned tasks. It outlines the deliverables that were produced; it describes the testing that was conducted on the system and explains the problems that were encountered but have yet to be addressed; it suggests configurations suitable for future demonstrations; and it discusses shortcomings and improvements to the system design.

[1] Note that inter-domain policies may also be intra-organizational policies as some "domains" will be identified parts of larger organizations.

3. Deliverables

3.1 Design Documents

The project team produced three design documents as follows:

"Policy Based Network Management – System Design Document" - [PBNM]

"Policy Decision Point (PDP) – Software Design Document" - [PDP]

"Policy Negotiation Proxy (PNP) – Software Design Document" - [PNP]

The [PBNM] document presents an architecture and system level design for a generic PBNM framework that supports policy negotiation. The proposed system facilitates the compilation of policies, the storage of policies, the exchange of policies, the evaluation and negotiation of policies, as well as the implementation and enforcement of policies. The [IDSP] document provides a detailed specification for negotiable inter-domain security policies. The proposed system can also support static policies such as Quality of Service (QoS) policies, which are implemented directly within the local administrative domain and do not require negotiation.

The [PDP] document presents a software design for the Policy Decision Point (PDP) component of PBNM system described in [PBNM]. The system facilitates the compilation of policies, the storage of policies, the exchange of policies, the evaluation and negotiation of policies, as well as the implementation and enforcement of policies.

The [PNP] document presents a software design for the Policy Negotiation Proxy (PNP) component of PBNM system described in the [PBNM]. The system facilitates the exchange and negotiation of policies on behalf of the Policy Decision Point (PDP) component.

The PBNM system includes an additional component called the Policy Editor [IDPE] that was developed as part of an earlier DRDC initiative. The Policy Editor edits and validates inter-domain security policies and submits them to the PDP.

3.2 PBNM Software

The PBNM system, which includes the Policy Editor, PDP and the PNP, is implemented in Java. The PBNM system includes approximately 17,500 lines of Java code. The PDP and PNP components include approximately 12,000 lines of Java code, while the Policy Server, implemented under Task 11, comprises almost 5,500 lines of Java code. Moreover, the UMU COPS implementation adds an additional 11,000 lines of Java code to the PBNM system. Details regarding the design of the policy server, as well as the integration of UMU COPS, can be found in [PDP].

The primary goal of the project team was to create an extensible PBNM framework that could support different types of policies without requiring significant modifications to the existing software. The only software component that possesses knowledge of policy structure, syntax and encoding resides within the PDP and is called the *Policy Processing Unit* (PPU). The PDP requires the implementation of a distinct *PPU* class for each type of policy supported by the system. The [PDP] design document describes how a specific *PPU* class for negotiable inter-domain security policies was implemented by extending a pair of abstract Java classes.

The current PBNM system supports the negotiation of inter-domain security policies, resulting in the generation of a Merged Policy object. The *IDSecurityPolicyPPU* class must separate the information contained within this Merged Policy object based on PEP device type or role and submit the information to the *Policy Server* for dissemination to PEP devices.

The command interface between the PDP Main program and the *PPU* was not implemented. Although not a functional component of the PDP, the command interface is useful in providing PDP status information to the user. This status information may include the following:

- The negotiation state for each remote administrative domain.
- The validity period of the current Policy Refresh object for each remote administrative domain.
- The time when the last Policy Refresh object was received by each remote administrative domain.

3.3 Collaboration Environment

During the development of the PBNM system, NRNS developers on behalf of Defence R&D Canada (DRDC) collaborated with developers from the Communication Research Center (CRC) in Ottawa and the University of Murcia (UMU) in Spain. A secure collaboration environment consisting of a virtual private network (VPN) based on IPsec protocols was established between NRNS and CRC. This VPN was used to secure project related traffic such as the problem reporting and tracking system described in section 3.5 and the software revision control system described in 3.6.

3.4 Software Development Environment

The project team employed Java software development kit (SDK) version 1.5 as the base development environment, Eclipse [IDE] version 3.0.1 as the integrated development environment [IDE], and Java version 1.5 as the run-time environment. The project team made use of both Windows XP and Redhat Linux CORE 3 as development workstations. The Concurrent Versions System (CVS) server included on Linux CORE 3 along with the Eclipse built-in CVS plug-in provided the necessary concurrent versioning control required in multiple developer environments.

3.5 Problem Reporting and Tracking System

A “Problem Reporting and Tracking System” was established to track problems and change requests associated with the PBNM software.

Developers working on this project developed software within their own environment using their own computer and network facilities, which were protected by security devices such as firewalls and VPNs. A web based solution was sought since it would have little to no impact as most organizations allow web traffic in and out their network in an unrestricted manner.

The Bugzilla [BUGZILLA] bug tracking system was selected as the problem reporting and tracking system for the PBNM Project. Bugzilla is a web application which allows multiple developers to create and track problem reports. The Bugzilla server was implemented on a system located at CRC.

3.6 Development and Test Environment

Both NRNS (on behalf of DRDC) and CRC have established at least two PBNM development and testing environments, as described in [PBNM]. These environments gave developers an opportunity to test the PBNM system as they developed additional functionality.

A Concurrent Versions System (CVS) server was established at each of the NRNS and CRC sites to house the local software repository. A top-level CVS server, hosted at CRC, merged the DRDC and CRC developed software into a single release. This merged software release was periodically copied back to each organization's CVS server to allow for sharing of common code and to facilitate system integration testing. The organization that developed new software components controlled when the new software components were replicated to the top-level CVS server. This ensured that other partners only received code that was fully tested and integrated into the PBNM system.

3.7 Software Component Testing

The project team tested all major PDP and PNP software components in isolation to some extent using the JUnit test framework. Moreover, the project team conducted partial system testing by integrating two or more major components into a single test environment. This incremental approach to testing allowed numerous issues to be discovered and addressed prior to full system level testing.

4. Compliance with System Design

The software design described in [PDP] and [PNP] does not fully implement the PBNM system described in [PBNM]. Exceptions are documented in [PDP] and [PNP]. These missing features should be incorporated as part of future design iterations and implemented within the PDP and PNP systems.

5. System Testing: Two Domains

Figure 1 illustrates the PBNM system as tested in a lab environment between two administrative domains. Each administrative domain comprised of a single system that housed all three PBNM components: the PDP, the PNP and the Policy Editor. In a real environment, these PBNM components each would reside on separate systems. The AD1 system was a Windows XP system and the AD2 system was a Redhat Linux CORE 3 system. The test environment did not include the Apache Xindice XML database[2]. Instead, a Stub XML Repository implementation was loaded that retrieved the XML Trusted Authorities file and the XML Address Resolution Mapping file from the local file system.

[2] The Xindice XML database in conjunction with the PBNM XML Repository software component did not provide sufficient stability.

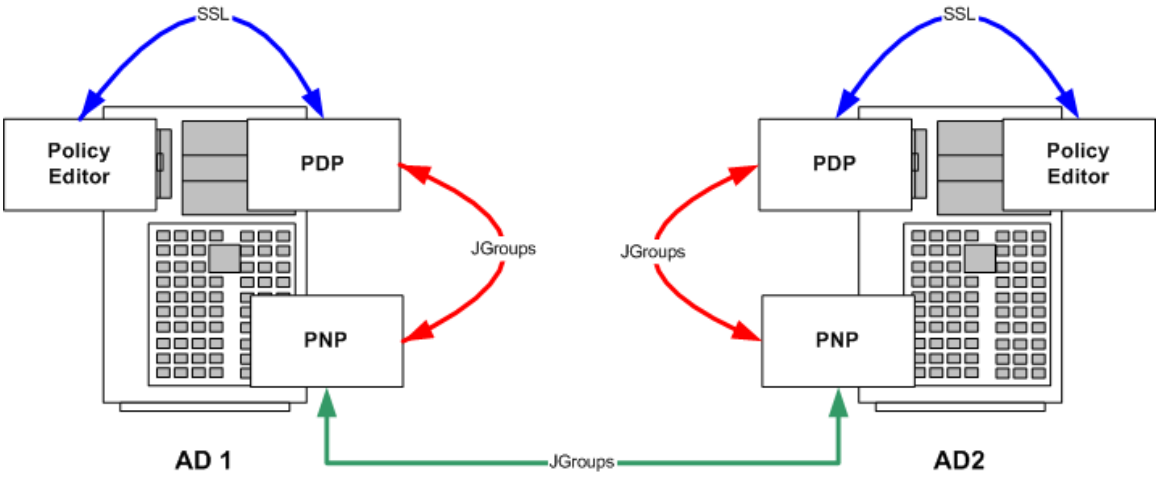

Figure 1 - Test Configuration

5.1 Test Scenarios

This section describes the test scenarios used as part of the system level testing between two administrative domains. Only simple policies were used to demonstrate the negotiation protocol and therefore the *IDSecurityPolicyPPU* class, which exceeds 3,000 lines of Java code, was not thoroughly tested as part of the system level testing. However, the *IDSecurityPolicyPPU* class underwent extensive JUnit testing. Lastly, since the system level testing only included two administrative domains, it was not possible to test administrative domain priorities.

5.1.1 Initial Policy Negotiation

The Policy Editor was used to create a policy for each administrative domain. Each administrative domain offered a specific service to the other administrative domain and each administrative domain expected a specific service from the other administrative domain.

All three PBNM components were started on each test system. The Policy Editor on each system was used to inject a policy to local PDP component. This caused a successful policy negotiation between AD1 and AD2, and the PDP on each system invoked the 'hook' to update the PEP configuration. Afterward, AD1 and AD2 exchanged periodic Policy Refresh objects to maintain the state of the negotiated policy.

5.1.2 Addition of a Local Service Requirement

The Policy Editor was used to add a non-critical Local Service Requirement to the policy for AD1.

The Policy Editor on AD1 was used to inject the modified policy to the PDP component on AD1. This caused a policy re-negotiation between AD1 and AD2. Since AD2 did not possess a matching Local Service Provision in its policy, it rejected AD1's newly added Local Service Requirement. However, because AD1 labelled the new Local Service Requirement as non-critical, the negotiation succeeded, and the PDP on each system

invoked the 'hook' to update the PEP configuration. Afterward, AD1 and AD2 exchanged periodic Policy Refresh objects to maintain the state of the negotiated policy.

5.1.3 Addition of a Local Service Provision

The Policy Editor was used to add a non-critical Local Service Provision to the policy for AD2.

The Policy Editor on AD2 was used to inject the modified policy to the PDP component on AD2. This caused a policy re-negotiation between AD1 and AD2. Since AD2 now possessed a matching Local Service Provision in its policy, both AD1 and AD2 accepted the other administrative domain's proposed policy in its entirety, and the PDP on each system invoked the 'hook' to update the PEP configuration. Afterward, AD1 and AD2 exchanged periodic Policy Refresh objects to maintain the state of the negotiated policy.

5.1.4 Removal of a Local Service Provision

The Policy Editor was used to remove the non-critical Local Service Provision from the policy for AD2.

The Policy Editor on AD2 was used to inject the modified policy to the PDP component on AD2. This caused a policy re-negotiation between AD1 and AD2. Since AD2 no longer possessed a matching Local Service Provision in its policy, it rejected AD1's recently added Local Service Requirement. However, because AD1 labelled the new Local Service Requirement as non-critical, the negotiation succeeded, and the PDP on each system invoked the 'hook' to update the PEP configuration. Afterward, AD1 and AD2 exchanged periodic Policy Refresh objects to maintain the state of the negotiated policy.

5.1.5 Removal of a Local Service Requirement

The Policy Editor was used to remove a non-critical Local Service Requirement from the policy for AD1. Both policies were now in their original form - each administrative domain offered a specific service to the other administrative domain and each administrative domain expected a specific service from the other administrative domain.

The Policy Editor on AD1 was used to inject the modified policy to the PDP component on AD1. This caused a successful policy negotiation between AD1 and AD2, and the PDP on each system invoked the 'hook' to update the PEP configuration. Afterward, AD1 and AD2 exchanged periodic Policy Refresh objects to maintain the state of the negotiated policy.

5.1.6 Extended Network Outage

The network connection between AD1 and AD2 was disconnected for an extended period of time. After the Policy Refresh object on each system expired, the PDP on each system invoked the 'hook' to update the PEP configuration. After the network connection was re-connected, AD1 and AD2 exchanged Policy Refresh objects to re-establish the previously negotiated policy state, and the PDP on each system invoked the 'hook' to update the PEP configuration. This demonstrated that the PBNM system can recover from an extended network outage without having to incur the full cost of a complete policy negotiation sequence.

5.2 Outstanding Problems

Some problems that were discovered during system level testing have yet to be addressed.

The PNP cannot properly handle interactions with more them one remote administrative domain. Errors in *PNPCore* class cause it to overwrite state information within its internal routing table.

The PNP drops policy negotiation units when delivered too quickly from the PDP. This occurs during a policy re-negotiation when the PDP transmits a Policy Proposal object quickly followed by a Negotiation Transcript object. The *PNPCore* class must queue outgoing policy negotiation units, since it manages the acknowledgements from the remote PNP. Currently, the *CommWorker* implementation queues policy negotiation objects.

Repository store operations to the Xindice XML database cause the calling PDP thread to block indefinitely from time to time. This problem could be attributed to the *XindiceRepository* class. Further investigation is needed to identify the exact source of this problem.

6. System Testing: Three Domains

NRNS completed some basic system level testing within a test environment that included three administrative domains (AD1, AD2, and AD3). All administrative domains included the other two administrative domains within their inter-domain security policy, resulting in successful negotiation between all parties and a fully-meshed environment. The main goal of the system level testing was to demonstrate that a Remote Service Restriction from a third party administrative domain can affect the negotiation with a lower priority administrative domain.

From the perspective of AD2, AD1 was assigned a higher priority than AD3. AD1 included a Remote Service Restriction that prevented AD2 from offering the TELNET service to any third party when AD2 was engaged with AD1. AD2 included a non-critical Local Service Provision that offered the TELNET service to AD3, and AD3 included a non-critical Local Service Requirement that required the TELNET service from AD2. When AD2 was engaged with AD1, AD2 did not offer the TELNET service to AD3. Since both AD2 and AD3 considered the TELNET service as non-critical, the policy negotiation between AD2 and AD3 succeeded without the provision of the TELNET service. When AD2 was not engaged with AD1, AD2 did offer the MAP service to AD3, the policy negotiation between AD2 and AD3 succeeded with the provision of the TELNET service to AD3 by AD2.

The project team created an automated process that periodically submitted a new policy to the AD1 PDP. The demonstration environment included two different policies for AD1 – one that contained the Remote Service Restriction for the TELNET service (Policy “1”) and one that did not contain the Remote Service Restriction for the TELNET service (Policy “2”). The automated process periodically submitted a new policy to the AD1 PDP – alternating between Policy “1” and Policy “2”.

When Policy “1” was active in AD1, AD2 was not providing the TELNET service to AD3. When Policy “1” was replaced with Policy “2” in AD1, AD1 would force AD2 to renegotiate its inter-domain security policy with AD1. Since the new policy from AD1 no longer contained the

Remote Service Restriction, AD2 would engage AD3 to renegotiate its inter-domain security policy and offer the TELNET service to AD3.

When Policy "2" was active in AD1, AD2 was providing the TELNET service to AD3. When Policy "2" was replaced with Policy "1" in AD1, AD1 would force AD2 to renegotiate its inter-domain security policy with AD1. Since the new policy from AD1 contained the Remote Service Restriction, AD2 would engage AD3 to renegotiate inter-domain its security policy but not offer the TELNET service to AD3.

This test scenario was successful in demonstrating how Remote Service Restrictions mandated from a higher priority administrative domain affected the policy negotiation with a lower priority administrative domain. Although the use of Remote Service Restrictions may be interesting from a research perspective, it is not clear if such a mechanism would be useful or even desirable in an operational environment.

The inter-domain security policies used to execute the three domain test scenarios are included in Annex A of this document.

7. Design Shortcomings and Improvements

The PBNM system includes several shortcomings that should be addressed in the future. This section also includes suggestions for improving the PBNM system. These shortcomings and improvements should be addressed as part of future design iterations and implemented within the PDP and PNP systems.

7.1 Improved Extensibility

The PBNM software design makes use of Java interfaces to promote extensibility. This allows for different implementations of the same software component to be substituted into the system without affecting the remainder of the system. However, since the Main program must instantiate the implementing classes, the Main program needs to be modified to substitute a different software component into the system. Instead, the Main program should acquire the name of the implementing class from its configuration file and use Java reflection[3] to instantiate the class. In order to achieve this, the class constructors require uniformity in their signature, which cannot be guaranteed by the interface definition[4]. Instead, the interface for the major software components should include an init() method that mandates the parameter list required to initialize the software component.

7.2 PNP Restart

The *PNPHandler* accepts control Policy Negotiation Units (PNUs) from *PPU* objects to engage and disengage from remote administrative domains and uses this information to create an internal routing table. The *PNPHandler* forwards slightly modified versions of control PNUs to the PNP. If the PNP system restarts, it lacks the information needed to engage with other PNP devices in remote administrative domains. The PDP and PNP must closely monitor the state of their communication channel. When the communication channel is lost and re-established, the *PNPHandler* should retransmit a control PNU to the PNP for each entry in the *PNPHandler* internal routing table.

[3] Java reflection allows the instantiation of an object without knowing the class name at run-time.
[4] Java does not permit Interface definitions to include signature for class constructors.

7.3 Policy Negotiation Object Validity Period

The validity period for various policy negotiation objects should be configured on a per-site basis in the XML Address Resolution Mapping file. Currently, a uniform value is specified in the PDP configuration file.

7.4 Policy Refresh Object Validity Period

The PDP system should negotiate the validity period for Policy Refresh objects[5] with its peers. The PDP peers should select the shorter period being proposed by each system, but some bounds checking should be introduced to ensure that the remote system does not force the local system to transmit its Policy Refresh objects at an unacceptable rate that can lead to system or network resource depletion.

7.5 Health Monitoring

The PNP system transmits Policy Refresh objects numerous times within the lifetime stated by their validity period. This practice provides a basic form of health monitoring between two administrative domains. The PDP system should also negotiate the transmit rate for Policy Refresh objects with its peers and communicate this information to the PNP.

7.6 PNU Retransmit Interval

The PNP acknowledges each PNU received from a remote PNP. If the PNP does not receive the acknowledgement within a predefined time period, it retransmits the PNU. Some sites may connect via high-speed land lines, while other sites may connect through satellite links. A uniform PNU retransmit interval may not be suitable for all remote administrative domains. Like the validity period for various policy negotiation objects, the PNU retransmit interval also should be specified on a per-site basis in the XML Address Resolution Mapping file.

7.7 PNU Retransmit Interval

The PDP sets a reminder when a negotiation sequence is restarted or when a Policy Refresh object for a remote administrative domain expires. When this reminder is triggered, the PDP removes any policy information associated with the remote administrative domain from the PEP configuration. The duration of is reminder should be a multiple of the PNU retransmit timer for the remote administrative domain. This allows the PDP to be more tolerant of administrative domains interconnected by slower network links.

7.8 High-Level Construct Mapping

When the Policy Server is designed and implemented, a mechanism is needed to map high-level constructs such as Security Class names and Service names contained in the policy negotiation objects to lower-level constructs understood by PEP devices.

7.9 Command Interface

The PBNM system would benefit from a command interface between the PDP Main program and the *PPU.* Although not a functional component of the PDP, the command interface is useful in providing PDP status information to the user.

[5] The proposed Policy Refresh validity period should be included in the Policy Proposal object.

8. Conclusions

The PBNM system is a highly extensible PBNM framework that can support different types of policies. The *PPU* is the only PBNM software component that possesses knowledge of policy structure, syntax and encoding. The PDP requires the implementation of a distinct *PPU* class for each type of policy supported by the system. The PBNM system includes a distinct *PPU* class for negotiable inter-domain security policies.

The PDP and PNP components of the PBNM system include most of the functionality described in the [PBNM] and system level testing demonstrated the successful implementation of the policy negotiation protocol. Since only simple policies were used to demonstrate the negotiation protocol, the *IDSecurityPolicyPPU* class was not thoroughly tested as part of the system level testing.

The specification [PBNM] for inter-domain security policies describes how these policies are evaluated and negotiated. The specification is quite complex. The motive for compiling the inter-domain security policy specification was to create a requirements specification to assist in the design of a negotiated *PPU* for the PBNM system. It is not yet certain whether the specified inter-domain security policy is useful in an operational environment. Inter-domain security policies must be tested using complex policies in environments consisting of numerous administrative domains. Only then can the usefulness of the specification be evaluated and the accuracy of its implementing class be assessed.

Before more complex testing of the system can proceed, the problems associated with the PNP and the *XindiceRepository* must be addressed. The PNP must support simultaneous interactions with multiple remote PNP devices and the PDP must store and retrieve policy documents and objects from the Policy Repository.

References

[PBNM] "Policy Based Network Management – System Design Document", Version 1.1, NRNS Incorporated, September 2005

[PDP] "Policy Decision Point (PDP) – Software Design Document", Version 1.1, NRNS Incorporated, September 2005

[PNP] "Policy Negotiation Proxy (PNP) – Software Design Document", Version 1.0, NRNS Incorporated, March 2005

[IDPE] "Inter-Domain Policy Editor - System Implementation', Version 1.1, NRNS Incorporated, August 2005

[IDSP] "Discussion Paper - Specification of Inter-Domain Security Policies", Version DRAF T 0.3, NRNS Incorporated, December 2004

[IDE] http://www.eclipse.org

[BUGZILLA] http://www.bugzilla.org/

Annex A Test Scenario Policies

Policy "1" for AD1

```
<?xml version="1.0" encoding="UTF-8"?>
<IDPolicy xmlns:x0="http://www.w3.org/2001/XMLSchema">
    <GlobalPolicyScope>
        <Name/>
        <Preamble>
            <Declaration>
                <SecurityClass>Class A</SecurityClass>
                <DomainName>nrns.ca</DomainName>
                <Network>
                    <Address>10.10.10.0</Address>
                    <Netmask>255.255.255.0</Netmask>
                </Network>
            </Declaration>
            <LocalPolicyControl>
                <LocalServiceProvisionPermission>
                    <Protocol>HTTP</Protocol>
                </LocalServiceProvisionPermission>
                <LocalServiceProvisionPermission>
                    <Protocol>SSH</Protocol>
                </LocalServiceProvisionPermission>
                <LocalServiceRequirementPermission>
                    <Protocol>POP</Protocol>
                </LocalServiceRequirementPermission>
                <LocalServiceRequirementPermission>
                    <Protocol>IMAP</Protocol>
                </LocalServiceRequirementPermission>
            </LocalPolicyControl>
        </Preamble>
        <CoalitionPolicyScope>
            <Name>Test</Name>
            <Preamble>
                <Declaration>
                    <SecurityClass>Class A</SecurityClass>
                    <DomainName>nrns.ca</DomainName>
                    <Network>
                        <Address>10.10.10.0</Address>
                        <Netmask>255.255.255.0</Netmask>
                    </Network>
                </Declaration>
                <LocalPolicyControl>
                    <LocalServiceProvisionPermission>
                        <Protocol>HTTP</Protocol>
                    </LocalServiceProvisionPermission>
                    <LocalServiceProvisionPermission>
                        <Protocol>SSH</Protocol>
                    </LocalServiceProvisionPermission>
                    <LocalServiceRequirementPermission>
                        <Protocol>POP</Protocol>
                    </LocalServiceRequirementPermission>
                    <LocalServiceRequirementPermission>
                        <Protocol>IMAP</Protocol>
                    </LocalServiceRequirementPermission>
                </LocalPolicyControl>
            </Preamble>
            <ADPolicyScope>
                <Name>AD2</Name>
                <Priority>150</Priority>
                <Preamble>
                    <RemotePolicyControl>
```

```
                    <Protocol>TELNET</Protocol>
                </RemotePolicyControl>
            </Preamble>
            <ServiceAccessRule>
                <LocalServiceRequirement>
                    <Protocol>POP</Protocol>
                    <Critical>false</Critical>
                    <Network>
                        <Address>10.10.10.0</Address>
                        <Netmask>255.255.255.0</Netmask>
                    </Network>
                </LocalServiceRequirement>
                <LocalServiceProvision>
                    <name>www</name>
                    <IPAddress>10.10.10.1</IPAddress>
                    <Protocol>HTTP</Protocol>
                    <Critical>false</Critical>
                </LocalServiceProvision>
            </ServiceAccessRule>
        </ADPolicyScope>
        <ADPolicyScope>
            <Name>AD3</Name>
            <Priority>100</Priority>
            <ServiceAccessRule>
                <LocalServiceRequirement>
                    <Protocol>IMAP</Protocol>
                    <Critical>false</Critical>
                    <Network>
                        <Address>10.10.10.0</Address>
                        <Netmask>255.255.255.0</Netmask>
                    </Network>
                </LocalServiceRequirement>
                <LocalServiceProvision>
                    <name>ras</name>
                    <IPAddress>10.10.10.5</IPAddress>
                    <Protocol>SSH</Protocol>
                    <Critical>false</Critical>
                </LocalServiceProvision>
            </ServiceAccessRule>
        </ADPolicyScope>
    </CoalitionPolicyScope>
</GlobalPolicyScope>
</IDPolicy>
```

Policy "2" for AD1

```
<?xml version="1.0" encoding="UTF-8"?>
<IDPolicy xmlns:x0="http://www.w3.org/2001/XMLSchema">
    <GlobalPolicyScope>
        <Name/>
        <Preamble>
            <Declaration>
                <SecurityClass>Class A</SecurityClass>
                <DomainName>nrns.ca</DomainName>
                <Network>
                    <Address>10.10.10.0</Address>
                    <Netmask>255.255.255.0</Netmask>
                </Network>
            </Declaration>
            <LocalPolicyControl>
                <LocalServiceProvisionPermission>
                    <Protocol>HTTP</Protocol>
                </LocalServiceProvisionPermission>
                <LocalServiceProvisionPermission>
                    <Protocol>SSH</Protocol>
                </LocalServiceProvisionPermission>
                <LocalServiceRequirementPermission>
                    <Protocol>POP</Protocol>
                </LocalServiceRequirementPermission>
                <LocalServiceRequirementPermission>
                    <Protocol>IMAP</Protocol>
                </LocalServiceRequirementPermission>
            </LocalPolicyControl>
        </Preamble>
        <CoalitionPolicyScope>
            <Name>Test</Name>
            <Preamble>
                <Declaration>
                    <SecurityClass>Class A</SecurityClass>
                    <DomainName>nrns.ca</DomainName>
                    <Network>
                        <Address>10.10.10.0</Address>
                        <Netmask>255.255.255.0</Netmask>
                    </Network>
                </Declaration>
                <LocalPolicyControl>
                    <LocalServiceProvisionPermission>
                        <Protocol>HTTP</Protocol>
                    </LocalServiceProvisionPermission>
                    <LocalServiceProvisionPermission>
                        <Protocol>SSH</Protocol>
                    </LocalServiceProvisionPermission>
                    <LocalServiceRequirementPermission>
                        <Protocol>POP</Protocol>
                    </LocalServiceRequirementPermission>
                    <LocalServiceRequirementPermission>
                        <Protocol>IMAP</Protocol>
                    </LocalServiceRequirementPermission>
                </LocalPolicyControl>
            </Preamble>
            <ADPolicyScope>
                <Name>AD2</Name>
                <Priority>150</Priority>
                <ServiceAccessRule>
                    <LocalServiceRequirement>
                        <Protocol>POP</Protocol>
                        <Critical>false</Critical>
                        <Network>
                            <Address>10.10.10.0</Address>
                            <Netmask>255.255.255.0</Netmask>
```

```
                    </Network>
                </LocalServiceRequirement>
                <LocalServiceProvision>
                    <name>www</name>
                    <IPAddress>10.10.10.1</IPAddress>
                    <Protocol>HTTP</Protocol>
                    <Critical>false</Critical>
                </LocalServiceProvision>
            </ServiceAccessRule>
        </ADPolicyScope>
        <ADPolicyScope>
            <Name>AD3</Name>
            <Priority>100</Priority>
            <ServiceAccessRule>
                <LocalServiceRequirement>
                    <Protocol>IMAP</Protocol>
                    <Critical>false</Critical>
                    <Network>
                        <Address>10.10.10.0</Address>
                        <Netmask>255.255.255.0</Netmask>
                    </Network>
                </LocalServiceRequirement>
                <LocalServiceProvision>
                    <name>ras</name>
                    <IPAddress>10.10.10.5</IPAddress>
                    <Protocol>SSH</Protocol>
                    <Critical>false</Critical>
                </LocalServiceProvision>
            </ServiceAccessRule>
        </ADPolicyScope>
    </CoalitionPolicyScope>
</GlobalPolicyScope>
</IDPolicy>
```

Policy for AD2

```
<?xml version="1.0" encoding="UTF-8"?>
<IDPolicy xmlns:x0="http://www.w3.org/2001/XMLSchema">
    <GlobalPolicyScope>
        <Name/>
        <Preamble>
            <Declaration>
                <SecurityClass>Class A</SecurityClass>
                <DomainName>drdc-rddc.gc.ca</DomainName>
                <Network>
                    <Address>10.10.20.0</Address>
                    <Netmask>255.255.255.0</Netmask>
                </Network>
            </Declaration>
            <LocalPolicyControl>
                <LocalServiceProvisionPermission>
                    <Protocol>POP</Protocol>
                </LocalServiceProvisionPermission>
                <LocalServiceProvisionPermission>
                    <Protocol>SMTP</Protocol>
                </LocalServiceProvisionPermission>
                <LocalServiceRequirementPermission>
                    <Protocol>HTTP</Protocol>
                </LocalServiceRequirementPermission>
                <LocalServiceRequirementPermission>
                    <Protocol>TELNET</Protocol>
                </LocalServiceRequirementPermission>
            </LocalPolicyControl>
        </Preamble>
        <CoalitionPolicyScope>
            <Name/>
            <Preamble>
                <Declaration>
                    <SecurityClass>Class A</SecurityClass>
                    <DomainName>drdc-rddc.gc.ca</DomainName>
                    <Network>
                        <Address>10.10.20.0</Address>
                        <Netmask>255.255.255.0</Netmask>
                    </Network>
                </Declaration>
                <LocalPolicyControl>
                    <LocalServiceProvisionPermission>
                        <Protocol>POP</Protocol>
                    </LocalServiceProvisionPermission>
                    <LocalServiceProvisionPermission>
                        <Protocol>SMTP</Protocol>
                    </LocalServiceProvisionPermission>
                    <LocalServiceRequirementPermission>
                        <Protocol>HTTP</Protocol>
                    </LocalServiceRequirementPermission>
                    <LocalServiceRequirementPermission>
                        <Protocol>TELNET</Protocol>
                    </LocalServiceRequirementPermission>
                </LocalPolicyControl>
            </Preamble>
            <ADPolicyScope>
                <Name>AD1</Name>
                <Priority>40</Priority>
                <ServiceAccessRule>
                    <LocalServiceRequirement>
                        <Protocol>HTTP</Protocol>
                        <Critical>false</Critical>
                        <Network>
                            <Address>10.10.20.0</Address>
                            <Netmask>255.255.255.0</Netmask>
```

```
                    </Network>
                </LocalServiceRequirement>
                <LocalServiceProvision>
                    <name>mail</name>
                    <IPAddress>10.10.20.1</IPAddress>
                    <Protocol>POP</Protocol>
                    <Critical>false</Critical>
                </LocalServiceProvision>
            </ServiceAccessRule>
        </ADPolicyScope>
        <ADPolicyScope>
            <Name>AD3</Name>
            <Priority>20</Priority>
            <ServiceAccessRule>
                <LocalServiceRequirement>
                    <Protocol>TELNET</Protocol>
                    <Critical>false</Critical>
                    <Network>
                        <Address>10.10.20.0</Address>
                        <Netmask>255.255.255.0</Netmask>
                    </Network>
                </LocalServiceRequirement>
                <LocalServiceProvision>
                    <name>smtp</name>
                    <IPAddress>10.10.20.2</IPAddress>
                    <Protocol>SMTP</Protocol>
                    <Critical>false</Critical>
                </LocalServiceProvision>
            </ServiceAccessRule>
        </ADPolicyScope>
    </CoalitionPolicyScope>
</GlobalPolicyScope>
</IDPolicy>
```

Policy for AD3

```
<?xml version="1.0" encoding="UTF-8"?>
<IDPolicy xmlns:x0="http://www.w3.org/2001/XMLSchema">
    <GlobalPolicyScope>
        <Name/>
        <Preamble>
            <Declaration>
                <SecurityClass>Class A</SecurityClass>
                <DomainName>crc.ca</DomainName>
                <Network>
                    <Address>10.10.30.0</Address>
                    <Netmask>255.255.255.0</Netmask>
                </Network>
            </Declaration>
            <LocalPolicyControl>
                <LocalServiceProvisionPermission>
                    <Protocol>IMAP</Protocol>
                </LocalServiceProvisionPermission>
                <LocalServiceProvisionPermission>
                    <Protocol>TELNET</Protocol>
                </LocalServiceProvisionPermission>
                <LocalServiceRequirementPermission>
                    <Protocol>SSH</Protocol>
                </LocalServiceRequirementPermission>
                <LocalServiceRequirementPermission>
                    <Protocol>SMTP</Protocol>
                </LocalServiceRequirementPermission>
            </LocalPolicyControl>
        </Preamble>
        <CoalitionPolicyScope>
            <Name/>
            <Preamble>
                <Declaration>
                    <SecurityClass>Class A</SecurityClass>
                    <DomainName>crc.ca</DomainName>
                    <Network>
                        <Address>10.10.30.0</Address>
                        <Netmask>255.255.255.0</Netmask>
                    </Network>
                </Declaration>
                <LocalPolicyControl>
                    <LocalServiceProvisionPermission>
                        <Protocol>IMAP</Protocol>
                    </LocalServiceProvisionPermission>
                    <LocalServiceProvisionPermission>
                        <Protocol>TELNET</Protocol>
                    </LocalServiceProvisionPermission>
                    <LocalServiceRequirementPermission>
                        <Protocol>SSH</Protocol>
                    </LocalServiceRequirementPermission>
                    <LocalServiceRequirementPermission>
                        <Protocol>SMTP</Protocol>
                    </LocalServiceRequirementPermission>
                </LocalPolicyControl>
            </Preamble>
            <ADPolicyScope>
                <Name>AD1</Name>
                <Priority>40</Priority>
                <ServiceAccessRule>
                    <LocalServiceRequirement>
                        <Protocol>SSH</Protocol>
                        <Critical>false</Critical>
                        <Network>
                            <Address>10.10.30.0</Address>
                            <Netmask>255.255.255.0</Netmask>
```

```
                    </Network>
                </LocalServiceRequirement>
                <LocalServiceProvision>
                    <name>Mail</name>
                    <IPAddress>10.10.30.5</IPAddress>
                    <Protocol>IMAP</Protocol>
                    <Critical>false</Critical>
                </LocalServiceProvision>
            </ServiceAccessRule>
        </ADPolicyScope>
        <ADPolicyScope>
            <Name>AD2</Name>
            <Priority>20</Priority>
            <ServiceAccessRule>
                <LocalServiceRequirement>
                    <Protocol>SMTP</Protocol>
                    <Critical>false</Critical>
                    <Network>
                        <Address>10.10.30.0</Address>
                        <Netmask>255.255.255.0</Netmask>
                    </Network>
                </LocalServiceRequirement>
                <LocalServiceProvision>
                    <name>RAS</name>
                    <IPAddress>10.10.30.8</IPAddress>
                    <Protocol>TELNET</Protocol>
                    <Critical>false</Critical>
                </LocalServiceProvision>
            </ServiceAccessRule>
        </ADPolicyScope>
    </CoalitionPolicyScope>
</GlobalPolicyScope>
</IDPolicy>
```

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. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

NRNS Incorporated
4043 Carling Avenue
Ottawa 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 or U) in parentheses after the title.)

Policy Based Network Management: Final Report (U)

4. AUTHORS (Last name, first name, middle initial)

Spagnolo, J., Cayer D.

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

September 2005

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

19

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

7

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 the address.)

DRDC Ottawa/NIO Section
3701 Carling Avenue
Ottawa K1A 0Z4

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)

15BF27

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 NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

DRDC Ottawa CR 2005-112

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

(x) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to 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), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

(U) This report describes the results of a series of tasks to design, develop and test a prototype policy based network management (PBNM) system. The report describes some test scenarios and specifies a number of areas for future enhancements.

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.)

Common Open Policy Service (COPS) protocol
Inter-domain security policy
Network Managament
Policy
Policy-based network management
Policy Decision Point (PDP)
Policy Editor
Policy enforcement
Policy Enforcement Point (PEP)
Policy negotiation
Policy Negotiation Proxy (PNP)
Policy object
Polic Processing Unit (PPU)
Policy repository
Security policy
System testing
Test scenarios
XML policy

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