

Policy Based Network Management

Dr. Adrian Waller, Thales Research & Technology (UK)

10 May 2004

INET 2004



Security for the pervasive computing world



Contents

- Network Management problems
- Security management in particular
- What is Policy Based Network Management ?
- How might PBNM help?
- Typical architectures
- Approaches to PBNM
- Advanced/Future issues
- Concluding remarks

The network management problem - 1

Wanted:

- System administrator for medium-sized company with the following skills:
 - ▲ NT, UNIX, Windows 2000, firewalls, IDS, Cisco routers, Linux, J2EE, .NET, XML, Apache Web server, IIS, IPsec, X. 509, IPv6, SSL, IKE, DNS, UDP, TCP, FTP, HTTP, SOAP, RPC, RMI, Java, C++, ASP, LDAP, OSPF, WLAN, SNMP, IntServ, DiffServ, CA, RA, Kerberos, Active Directory, Ethernet, PKI, VPN, NAT, RADIUS, VoIP, SIP, H. 323,.....

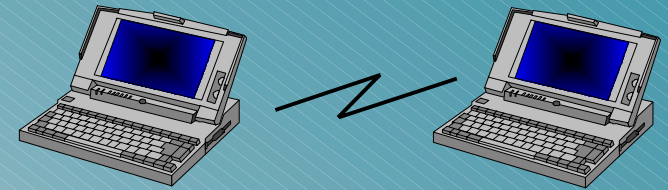
An impossible task ...



The network management problem - 2

Wanted:

- For a meeting at your site:
 - ▲ visitor access to Internet, some facilities & a network
- For your roaming workforce:
 - ▲ secure remote access to corporate network, from anywhere ...
- For your customer web site:
 - ▲ fast reliable access, even under load
- For a videoconference scheduled in 1 hour's time:
 - ▲ guaranteed quality of service for its duration



Anytime Anywhere. User expectations are growing ...

The network management problem - 3

Diverse selection of equipment and tools



Need for highly skilled network administrators

- ▲ Even then, still error prone

Convergence of communications & computing



Need for more dynamic, adaptable network facilities

- ▲ Adaptive use of limited resources (particularly for wireless networks)
- ▲ Context aware/application aware networks
- ▲ Ad hoc networks

What is Policy Based Network Management?

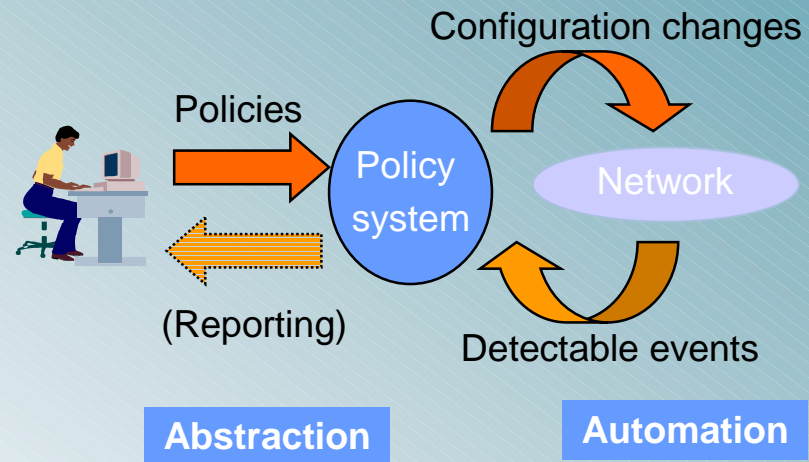
- PBNM is a condition - action response mechanism
 - ▲ to provide an automatic response to conditions in the network according to pre-defined policies
- and an abstraction/ translation mechanism
 - ▲ Define goals not device configurations
 - ▲ Changes in policy lead to changes in goals not implementations

Policies are 'rules' of the general form:

ON <event>

IF <conditions>

THEN <do actions>



Example Policies (high level)

- Deny internet access during business hours, or allow access only for a certain amount of time, or allow/deny certain web sites
- Allow specified group of users access to specified data directories on network, or certain services on network
- Allow priority use of network services for selected users/groups of users
- Allocate percentage of bandwidth to particular application
- Run local virus checking on every client every <N> minutes
- Virus check any transfer from floppy disk drive to hard drive

How might PBNM help?

Automating reactions which can be predefined

- ▲ if we already know what actions should be taken when an event or series of event happens
- ▲ reduces likelihood of human error & speeds up reaction time
- ▲ configuring large number of devices (e.g. PCs on network) with common policy

Translation of high level policy into low level device-specific configurations

- ▲ de-skills the task
- ▲ allows changes in policy without changing implementations
- ▲ matching organisational policy with enforcement technologies

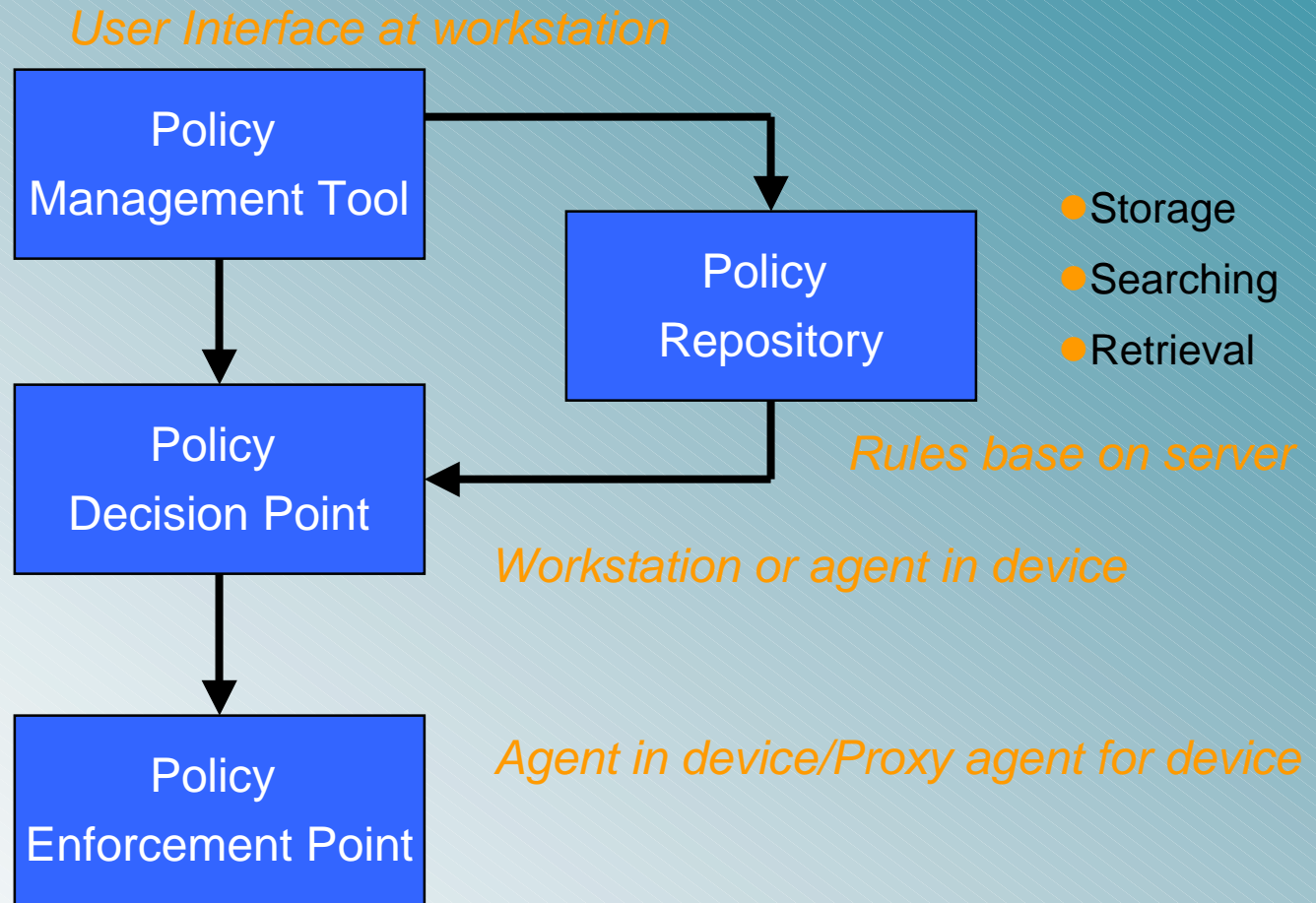
PBNM - typical architectural elements

- Creation
- Editing
- Validation
- Translation

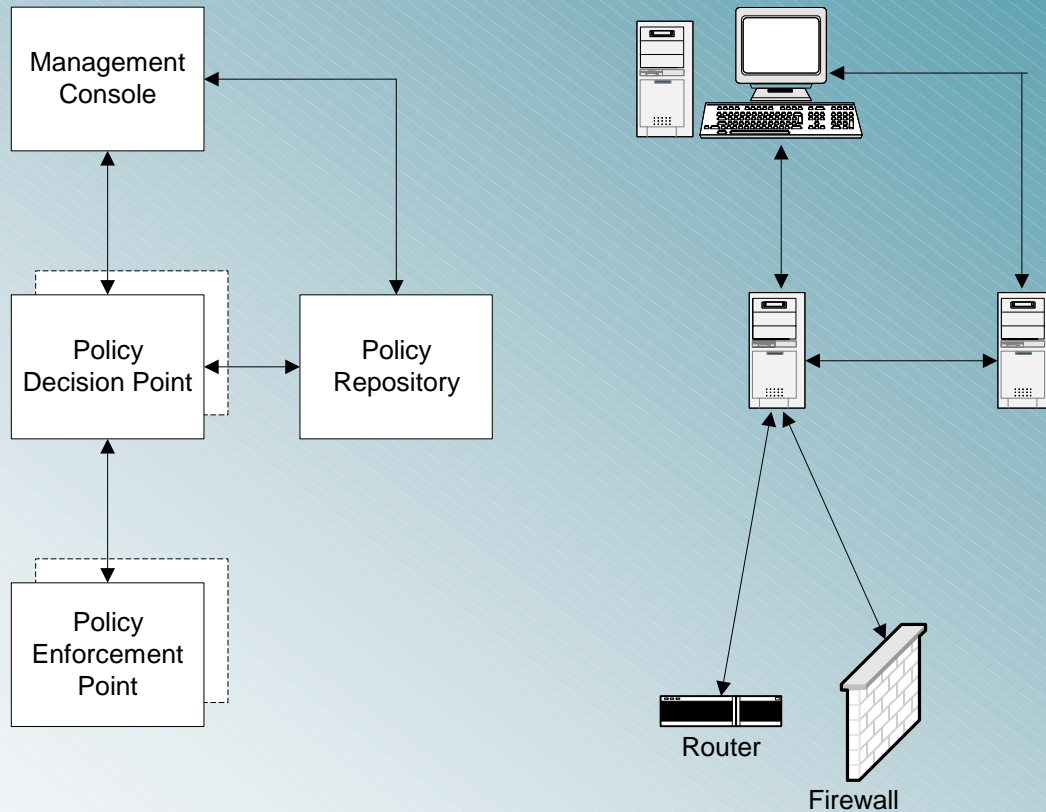
- Decisions
- Translation
- Configures

- Configures

- Storage
- Searching
- Retrieval



Typical architecture and deployment



(a) A logical PBNM Architecture

(b) An example deployment

Example deployment scenario

1. Define policy

2. Translate policy

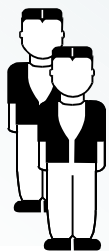
3. Deploy policy (*)
(auto or manual)

6. New policy decision
made and action applied
to network

4. Devices configured (*)

+ routers/switches/hubs *

5. Trigger event
happens



LAN users



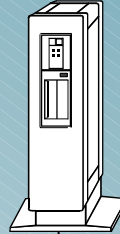
...



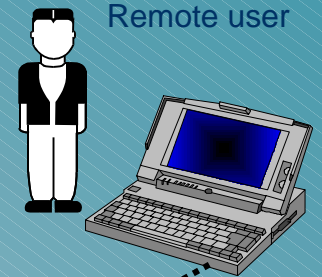
Administrator



Mail server



Remote user



Internet

Other office networks

Orange: Human

Blue: system

Typical architectural themes

There is diversity in PBNM systems. Common themes include:

- Different levels of policy specification

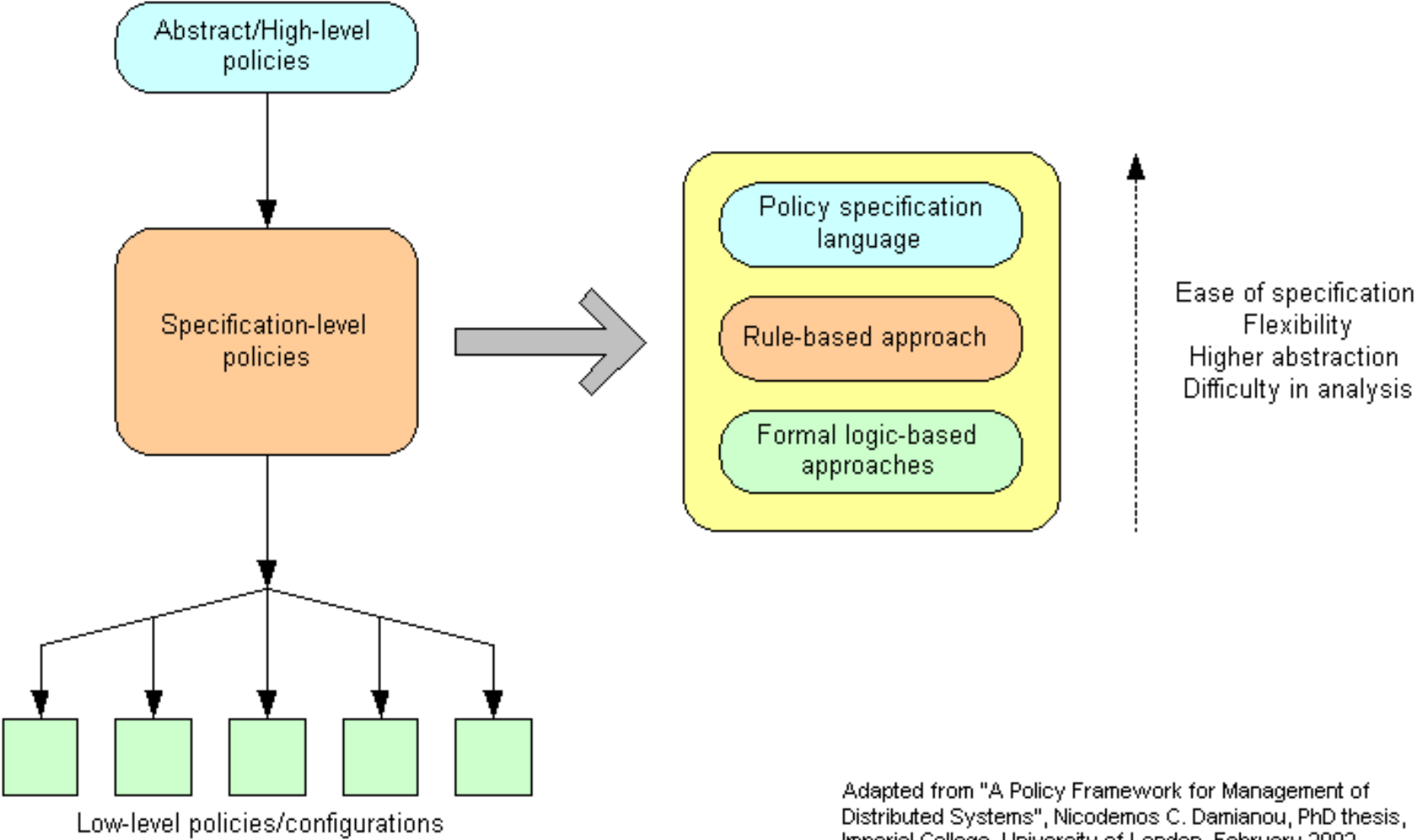
- ▲ At highest level, goals or service level agreements which have business meaning
- ▲ At lowest level, specific device configurations which can be implemented

- User interface or management console for creating, editing, & deploying policies and monitoring the results

- Protocols

- ▲ Desire for interoperable protocols between policy components, e.g. COPS, SNMP, LDAP, HTTP
- ▲ At lowest level must be device specific

Policy Translation



Policy Based Network Management, INET 2004 10/05/04

Adapted from "A Policy Framework for Management of Distributed Systems", Nicodemos C. Damianou, PhD thesis, Imperial College, University of London, February 2002.

Approaches to PBNM

▲
▲
▲
▲
▲ The terms 'Policy' and PBNM have a diverse meaning

▲ Approaches include:

▲ ■ Work in policy specification

▲ ▲ e.g. Ponder, XACML, KeyNote, IBM Trust Policy Language, IETF/DMTF Policy Core Information Model, ...

▲ ■ Work in protocols

▲ ▲ e.g. COPS, COPS-PR, ...

▲ ■ Commercial tools

▲ ▲ e.g. from Checkpoint, IBM Tivoli, Cisco, Allot Communications, Computer Associates, Orchestream, Intel, HP, Intelliden, Solsoft, Packeteer, Nortel, ...

▲ These are just a few examples ...
▲

Problems/future issues

Universal policy specification language/model

- Required so that common security policies can be mapped to multiple, heterogeneous implementations
 - ▲ e.g. a new device added to a network which doesn't support the current PBNM system. What do you do?
 - ▲ Configuration across administrative domains (interoperability)
- No agreement on such a language, and hard to produce one

Other policy related challenges remain:

- Resolving policy conflicts
- Automated refinement of policies from high-level to devices
- Policy validation
- Configuration correctness

Advanced security management

Delegation

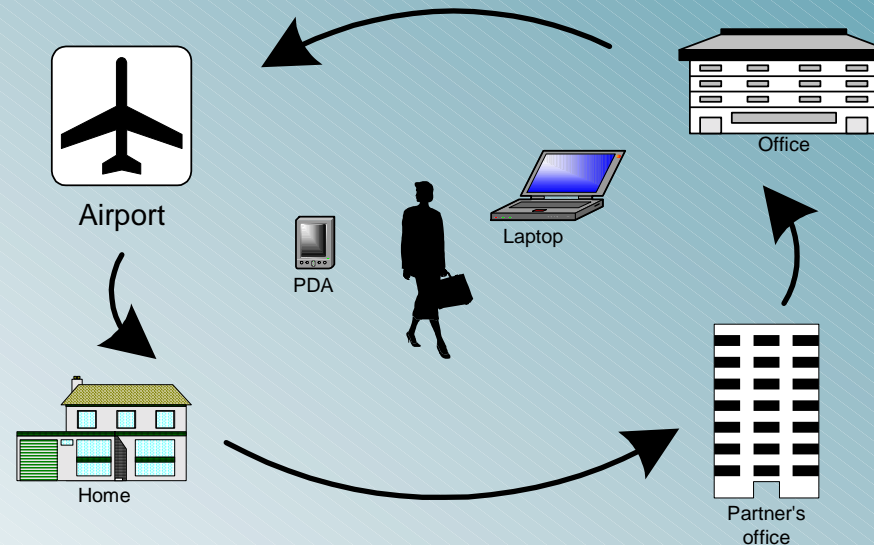
- Ability to assign, temporarily, rights to another user
 - ▲ Improves flexibility and scalability

Advanced access control policies

- Separation of duties (static and dynamic)
- Least privilege (RBAC and dynamic role assignment)
- Concurrency constraints (e.g. actions in a particular sequence, two particular roles can't be activated at same time)

Conclusions

- Pervasive mobile computing and communications are creating new security challenges



- PBNM could help solve these, and other network management issues
- There are solutions available but challenges remain and research continues in the difficult areas ...

More information

▲ Imperial College Policy Research Group Resources Page:

▲ <http://www-dse.doc.ic.ac.uk/Research/policies/resources.shtml>

▲ IETF Policy Framework Working Group:

▲ <http://www.ietf.org/html.charters/policy-charter.html>