Firewall Configuration Management Using XACML Policies

Asst. Prof. Dr. Tugkan TUGLULAR

Izmir Institute of Technology

Outline

- Problem Definition
- Proposed Architecture
- Firewall Configuration Management
- Prototype Implementation
- Experiments and Evaluation

Problem Definition

- Enterprise networks
  - multiple interconnected subnets distributed across various locations
- Firewalls are everywhere – subnets, PCs
  - focus on organizational policy level management instead of node level configuration
  - administered by different people with different views of security

Dynamic firewall configuration management required

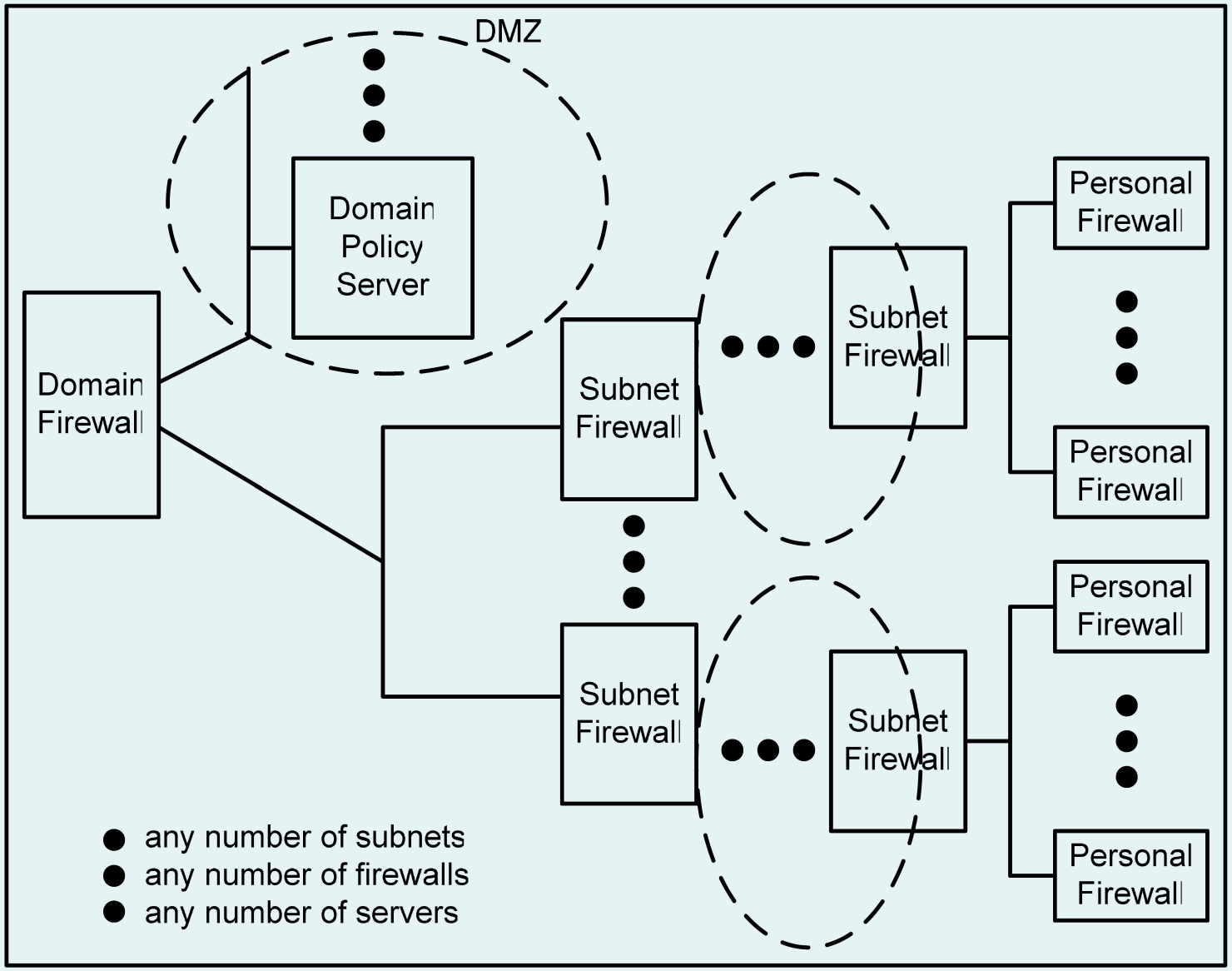
Proposed Solution

- Semi-distributed management
  - distribute organizational policies
  - enforce updated policies immediately
  - check for policy changes and anomalies
- XML based representation
  - policies, topology, communication, etc.

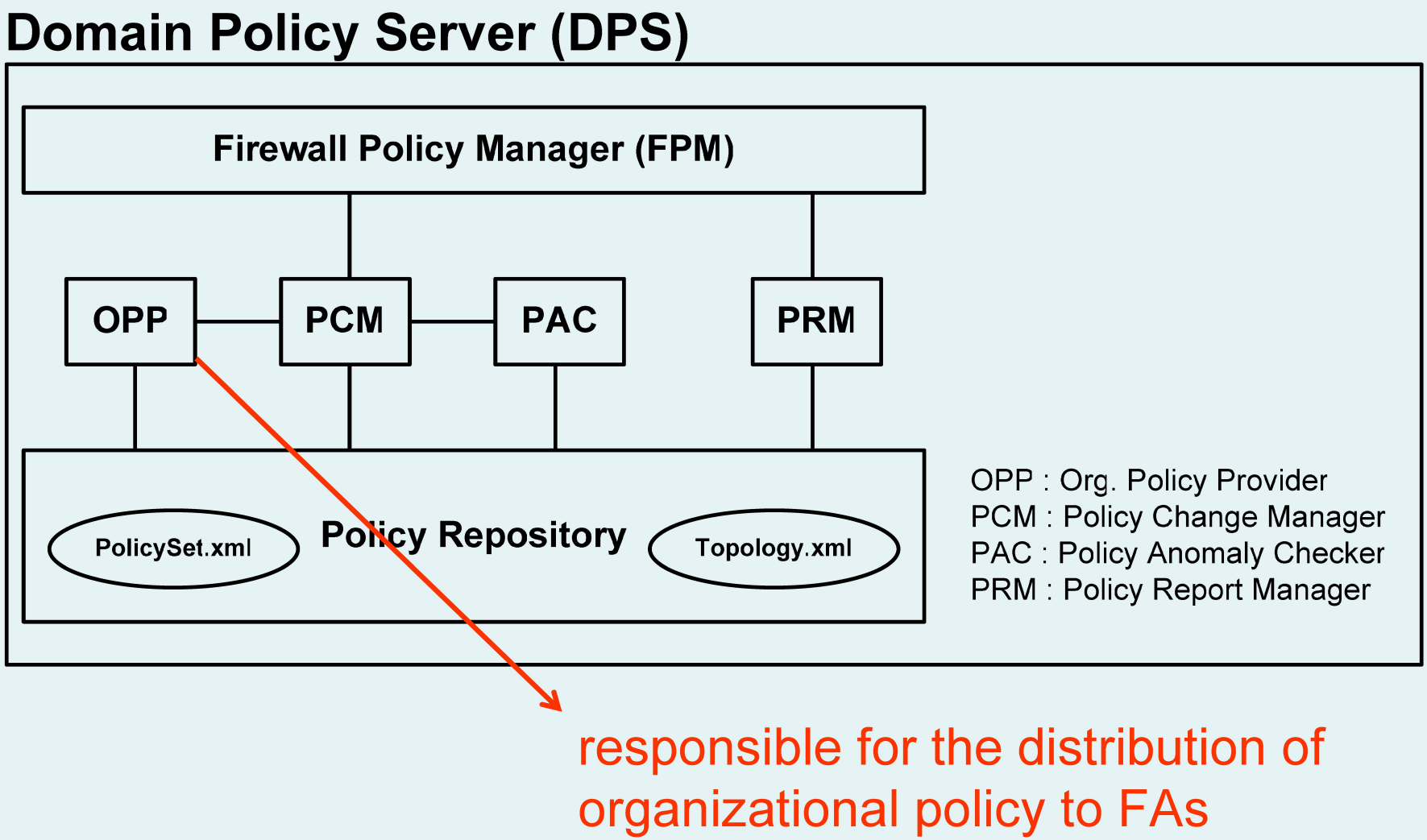
Firewall Configuration Management

- Firewall Configuration Management (FCM)
  - node level management
  - organizational policy propogated to lower nodes
- Dynamic firewalls
  - implementation neutral configuration
  - firewall agents

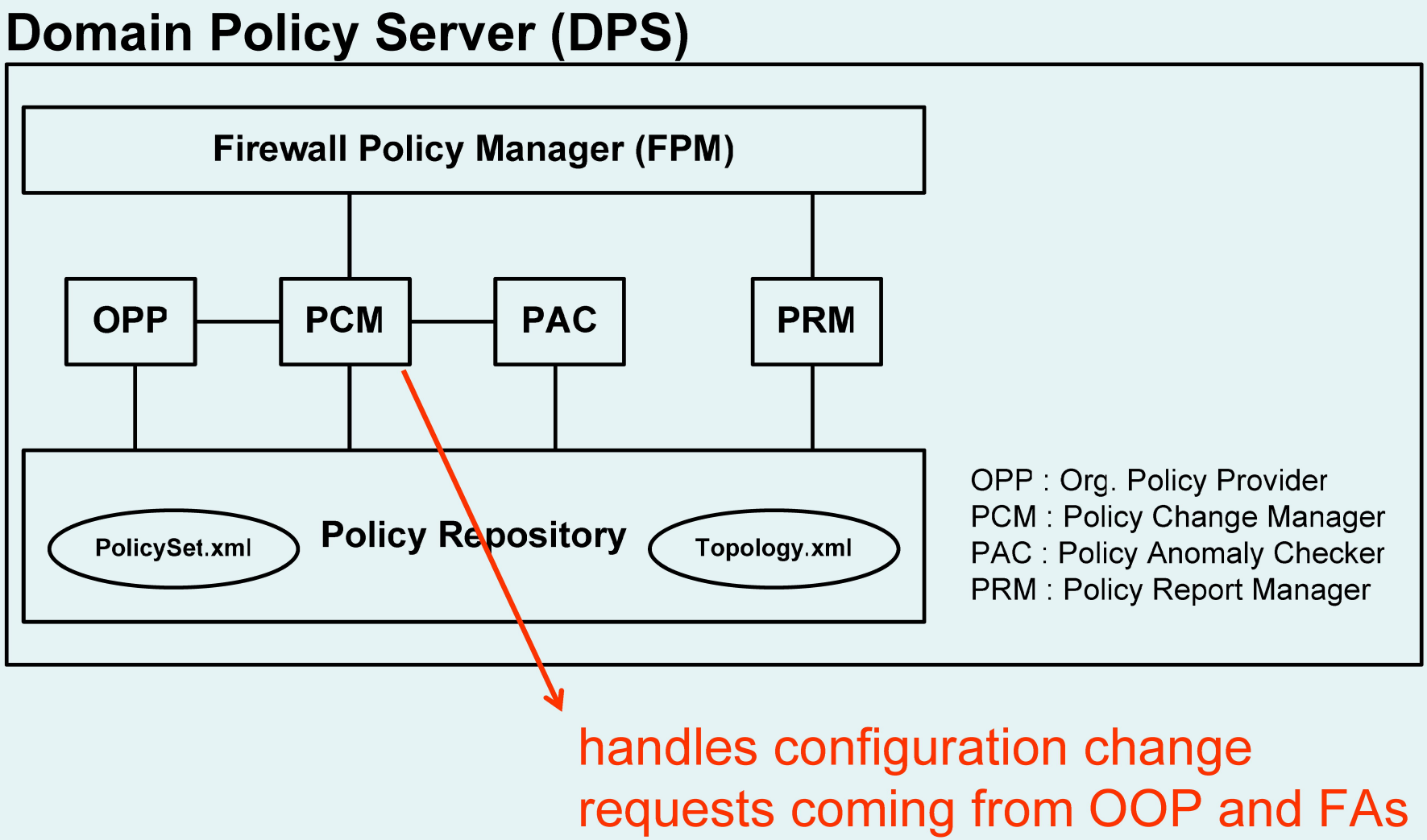
Network Domain Model



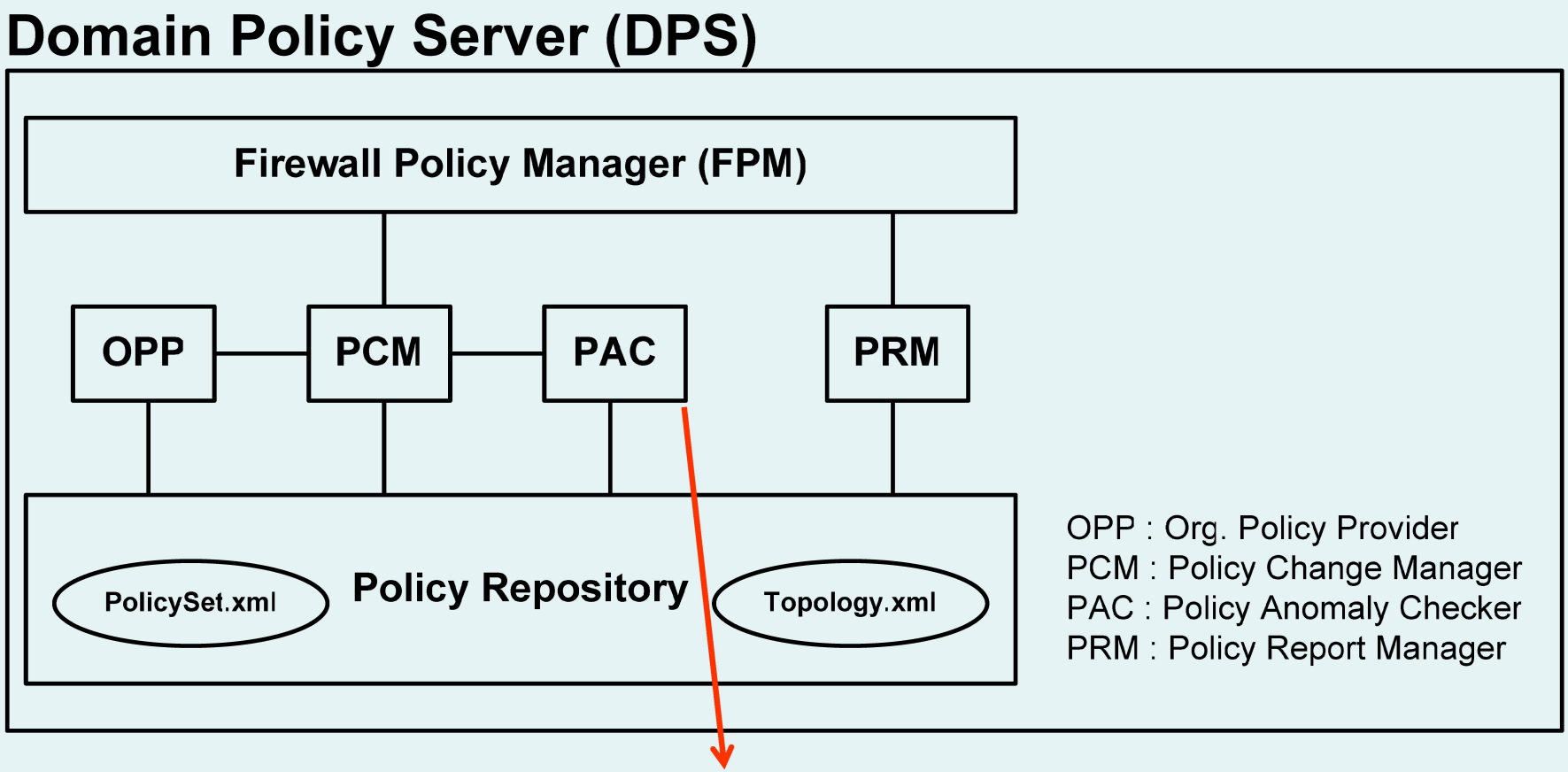
FCM Architecture



FCM Architecture

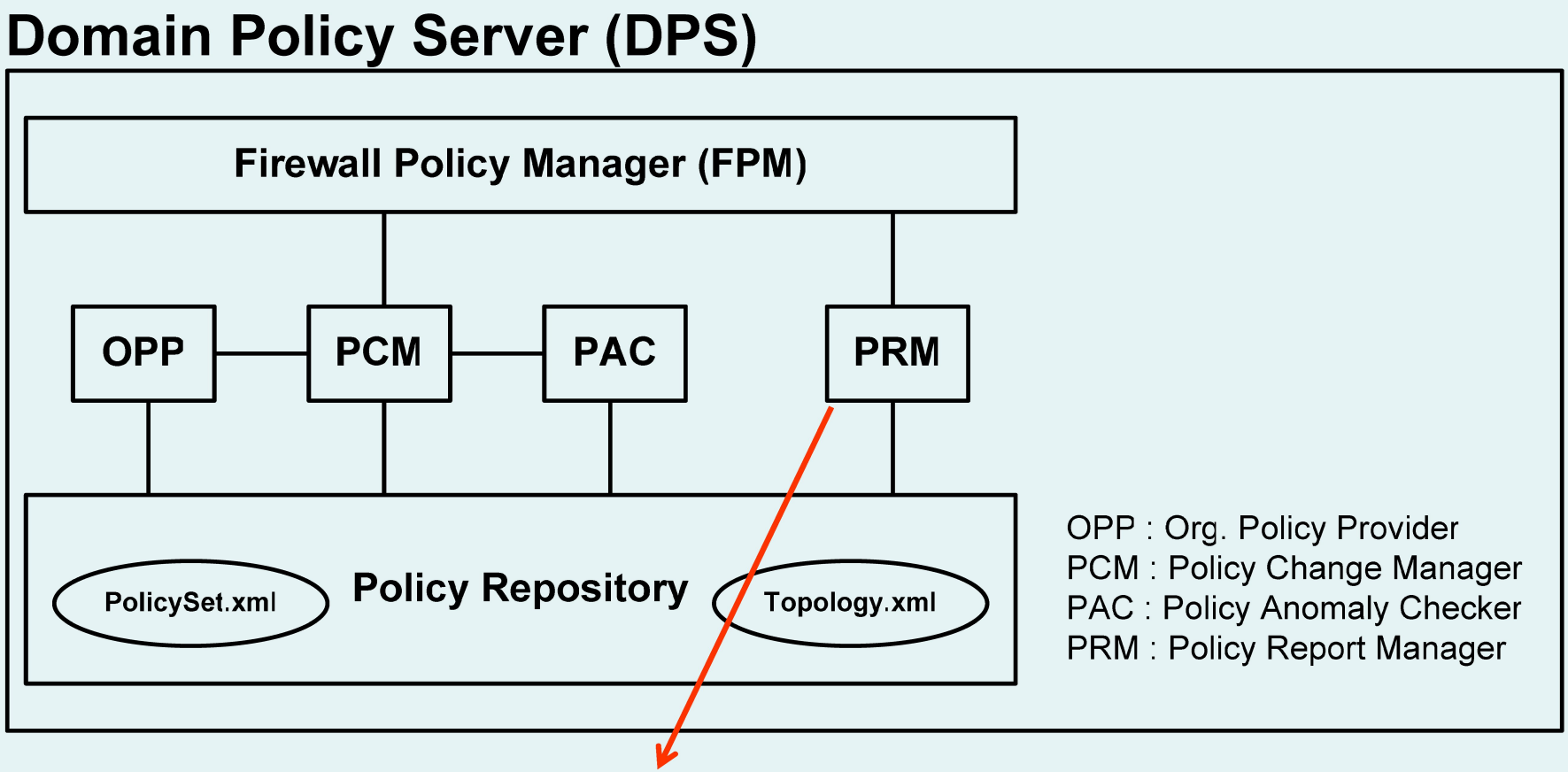


FCM Architecture



is not in conflict or inconsistent with the organizational policy as well as with the policies enforced enroute to domain firewall

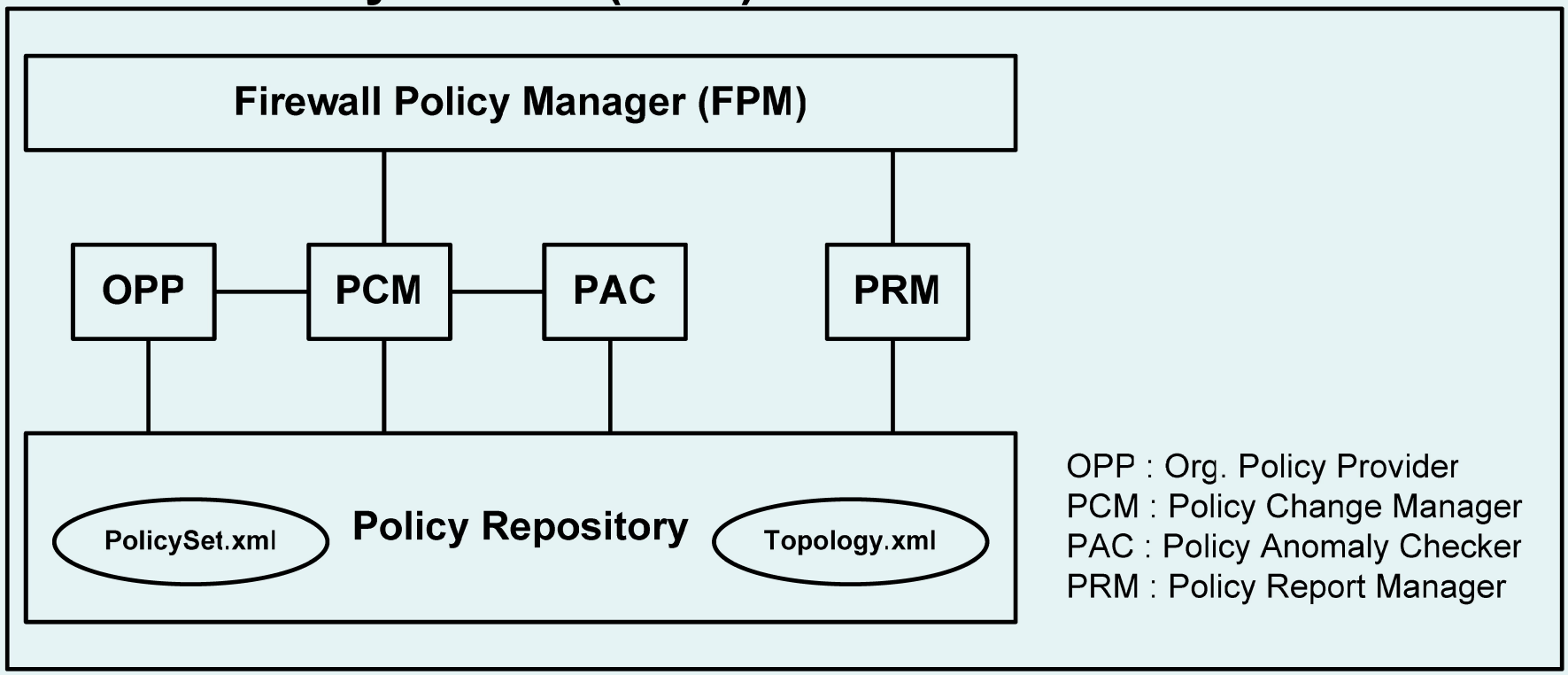
FCM Architecture



present topology, policy, and communication information on GUI

FCM Architecture

Domain Policy Server (DPS)



Firewall Agent (FA)

Iptables Firewall

Firewall Agent (FA)

- FA should be installed along with firewall
- Translation of implementation independent rules <order; protocol; src_ip; src_port; dst_ip; dst_port; action> to firewall commands and for their execution
- Subnet and personal firewalls expected to enforce both the organizational policy and its local policy
- Local policy should be consistent with policies of other firewalls that are enroute to domain firewall

XACML

- Specification of XML based Access Control Policies
- Sun's java based XACML implementation
- Java based UMU-XACML-Editor
- Extend it for firewall policies

XACML Rep. of Firewall Policy

- <Policy> all the rules of a firewall policy
- <Rule> a single rule of a firewall policy
- attributes of <Rule> order and action fields
- <Condition> protocol field
- <Subject> src_ip and src_port fields
- <Resource> dst_ip and dst_port fields

```
<?xml version="1.0"?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable"
PolicySetId="CampusPolicySet">
  <Description>Campus Network</Description>
...
  <Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" PolicyId="11"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
    <Description>Domain 11</Description>
    <Target />
    <Rule RuleId="4" Effect="Deny">
      <Description>tcp,155.223.64.*,*,193.140.248.162,80,deny</Description>
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:2.0:function:ipAddress-regexp-match">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">^(155)\.(223)\.(64)\.(25[0-
5]|2[0-4][0-9]|[01]?[0-9][0-9])\.(any)$</AttributeValue>
              <SubjectAttributeDesignator SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject" AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="urn:oasis:names:tc:xacml:2.0:data-type:ipAddress" />
            </SubjectMatch>
          </Subject>
        </Subjects>
        <Resources>
          <Resource>
            <ResourceMatch MatchId="urn:oasis:names:tc:xacml:2.0:function:ipAddress-regexp-match">
              <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">^(193)\.(140)\.(248)\.(162)\.(80)$</AttributeValue>
              <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="urn:oasis:names:tc:xacml:2.0:data-type:ipAddress" />
            </ResourceMatch>
          </Resource>
        </Resources>
      </Target>
      <Condition>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
            <SubjectAttributeDesignator AttributeId="protocol"
DataType="http://www.w3.org/2001/XMLSchema#string" />
          </Apply>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">tcp</AttributeValue>
        </Apply>
      </Condition>
    </Rule>
...
  </Policy>
..
</PolicySet>
```

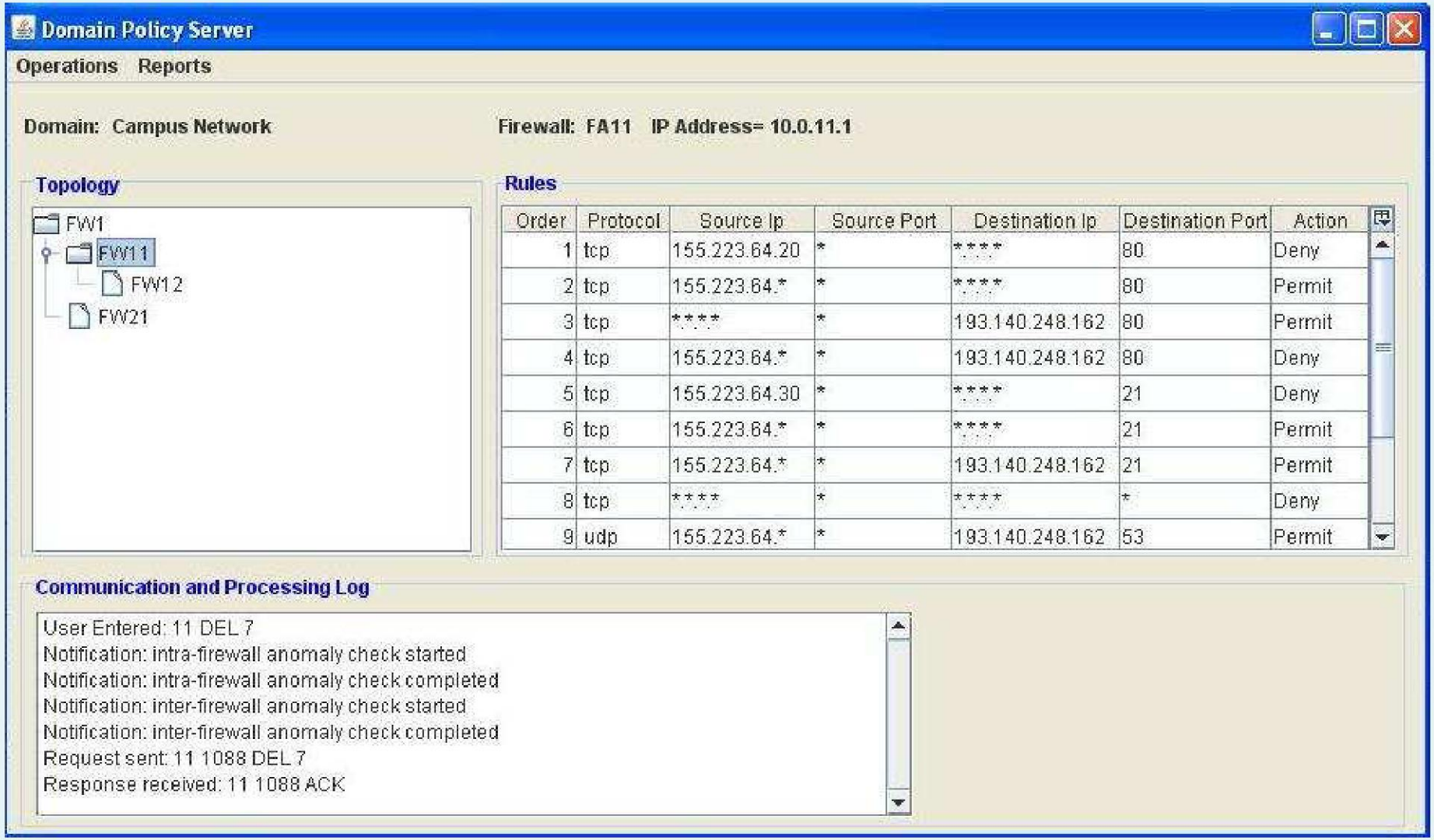
Configuration Messages

Direction	Command	Parameter	Explanation
FA → DPS	ADD	ordered-rule	add ordered-rule
FA → DPS	DEL	i	delete *ith* rule
DPS → FA	ADD	ordered-rule	add ordered-rule
DPS → FA	DEL	i	delete *ith* rule
DPS → FA	GET	i	get *ith* rule

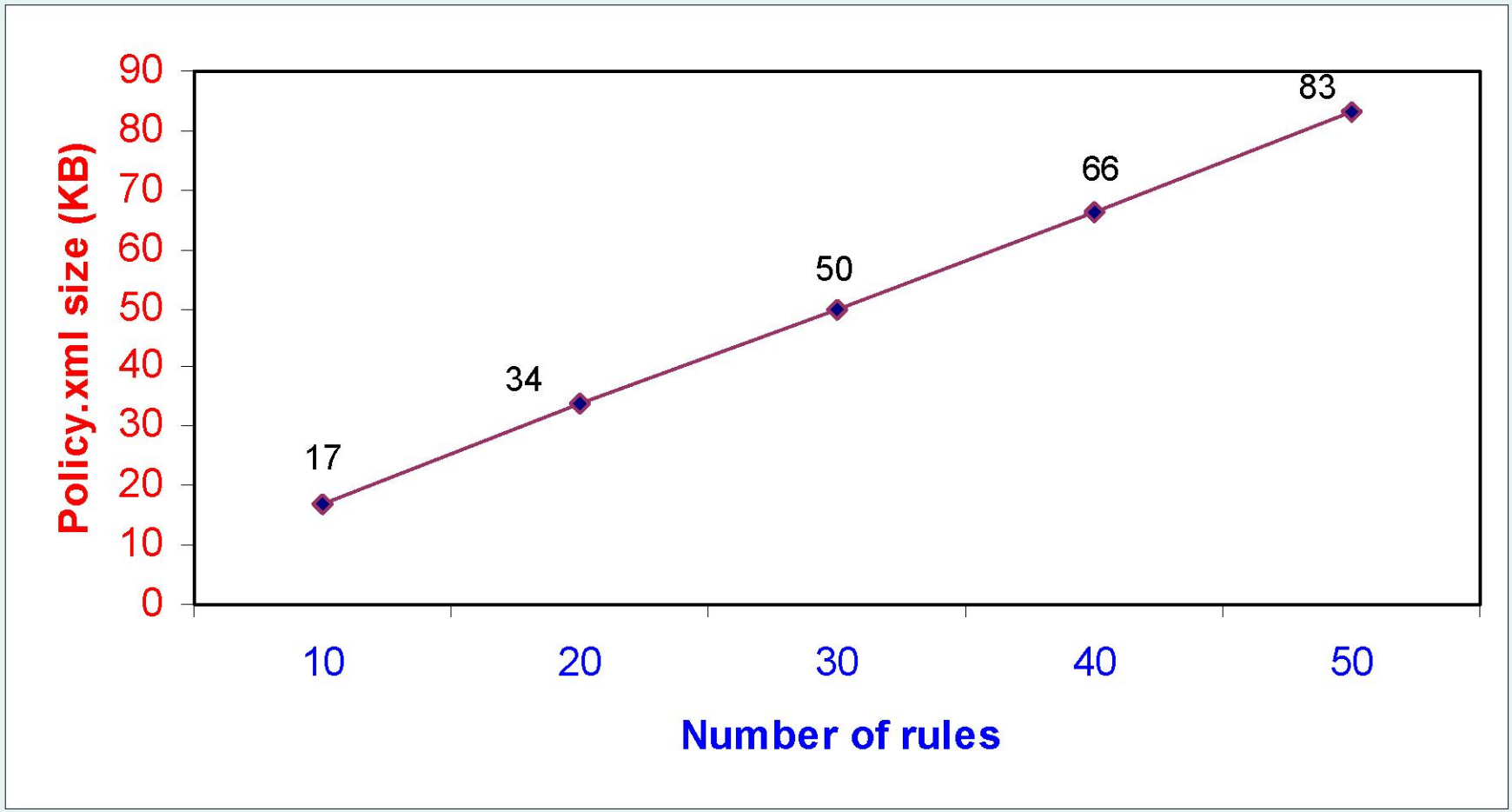
Configuration Messages

- Firewall configuration messages are in the form of a request and a response
- Request:
  - FA# SEQ# command {order | ordered-rule}
- Response:
  - FA# SEQ# ACK | NACK {ø | ordered-rule | exception}

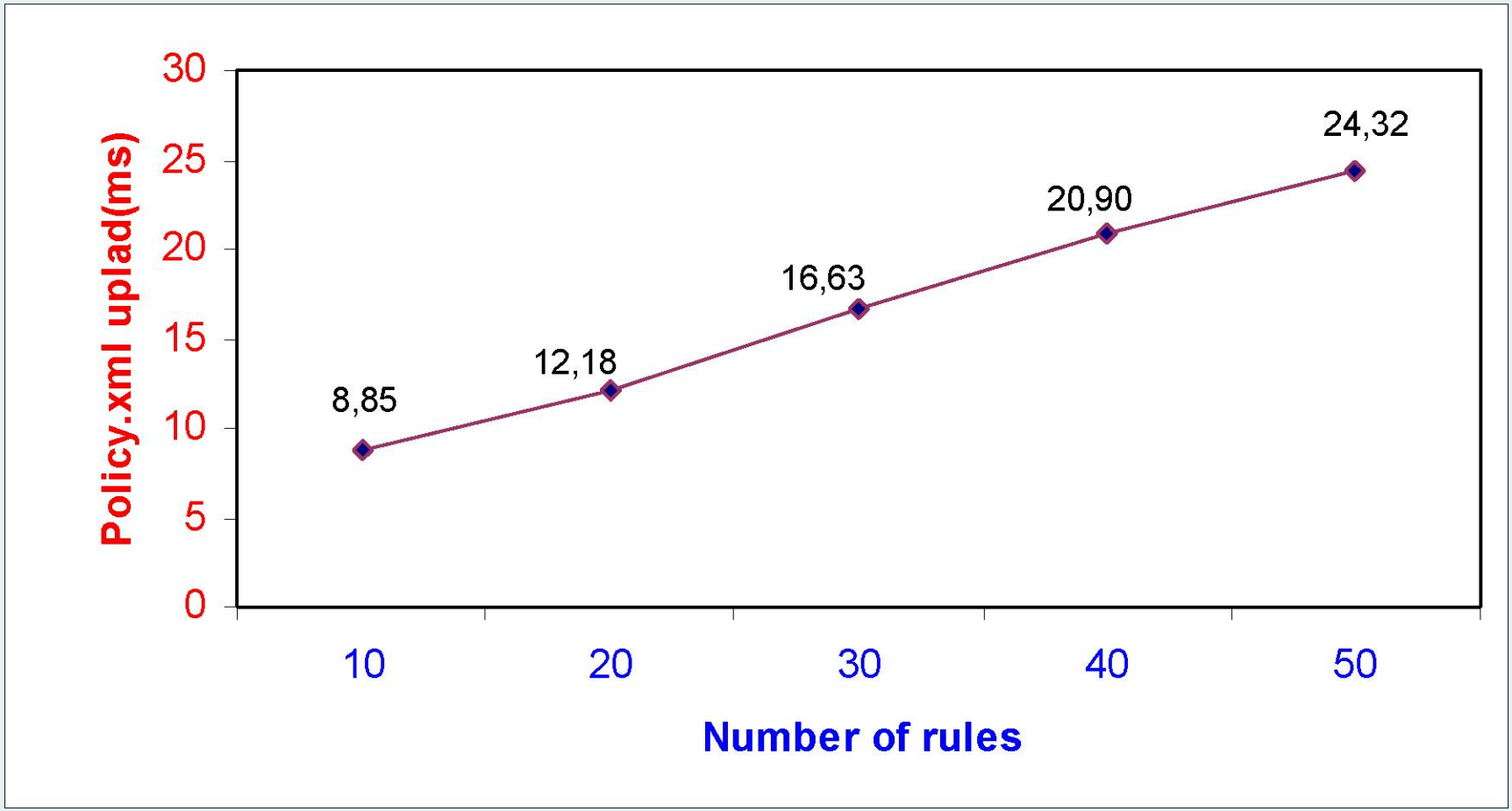
Prototype Implementation



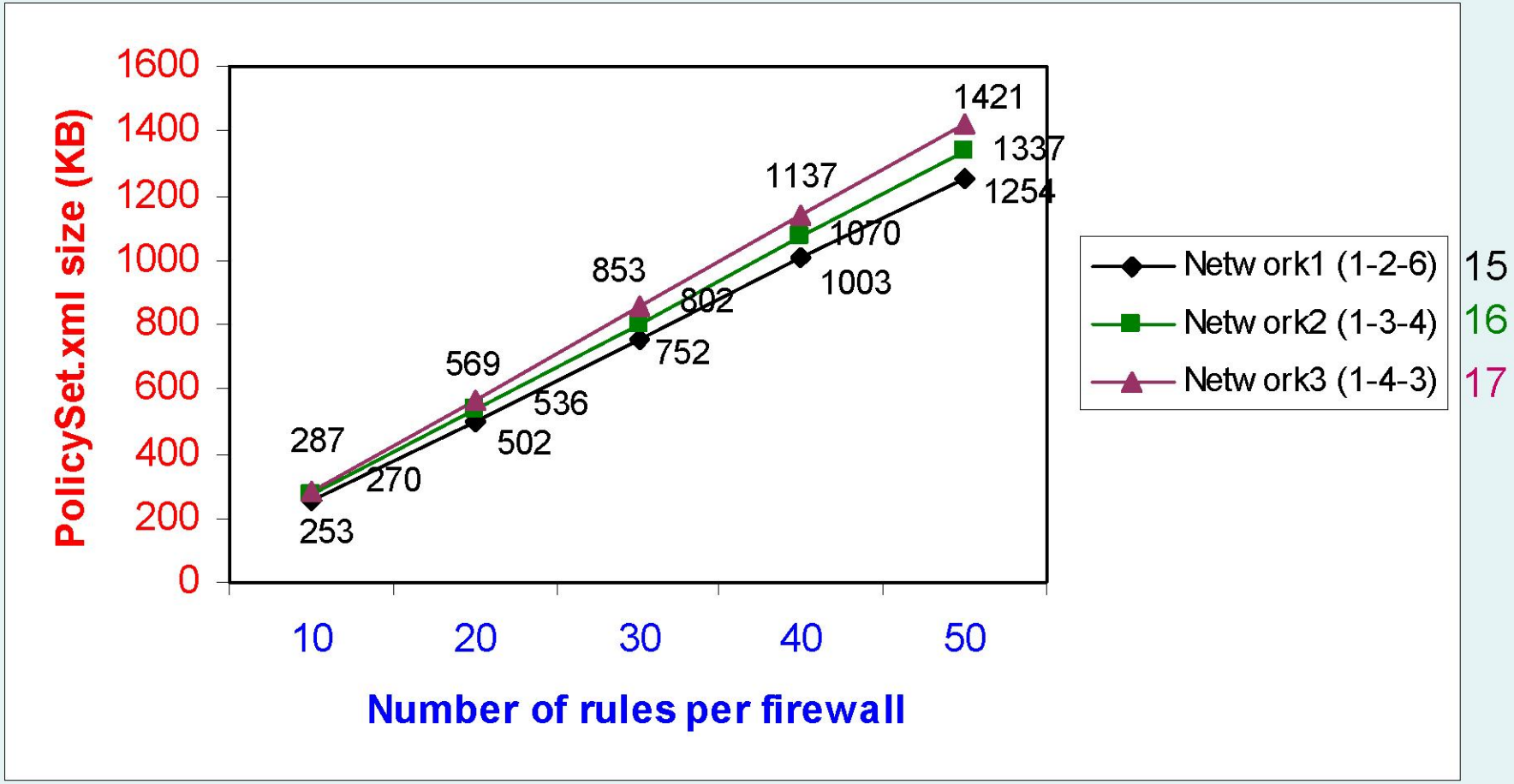
Operational Values - 1



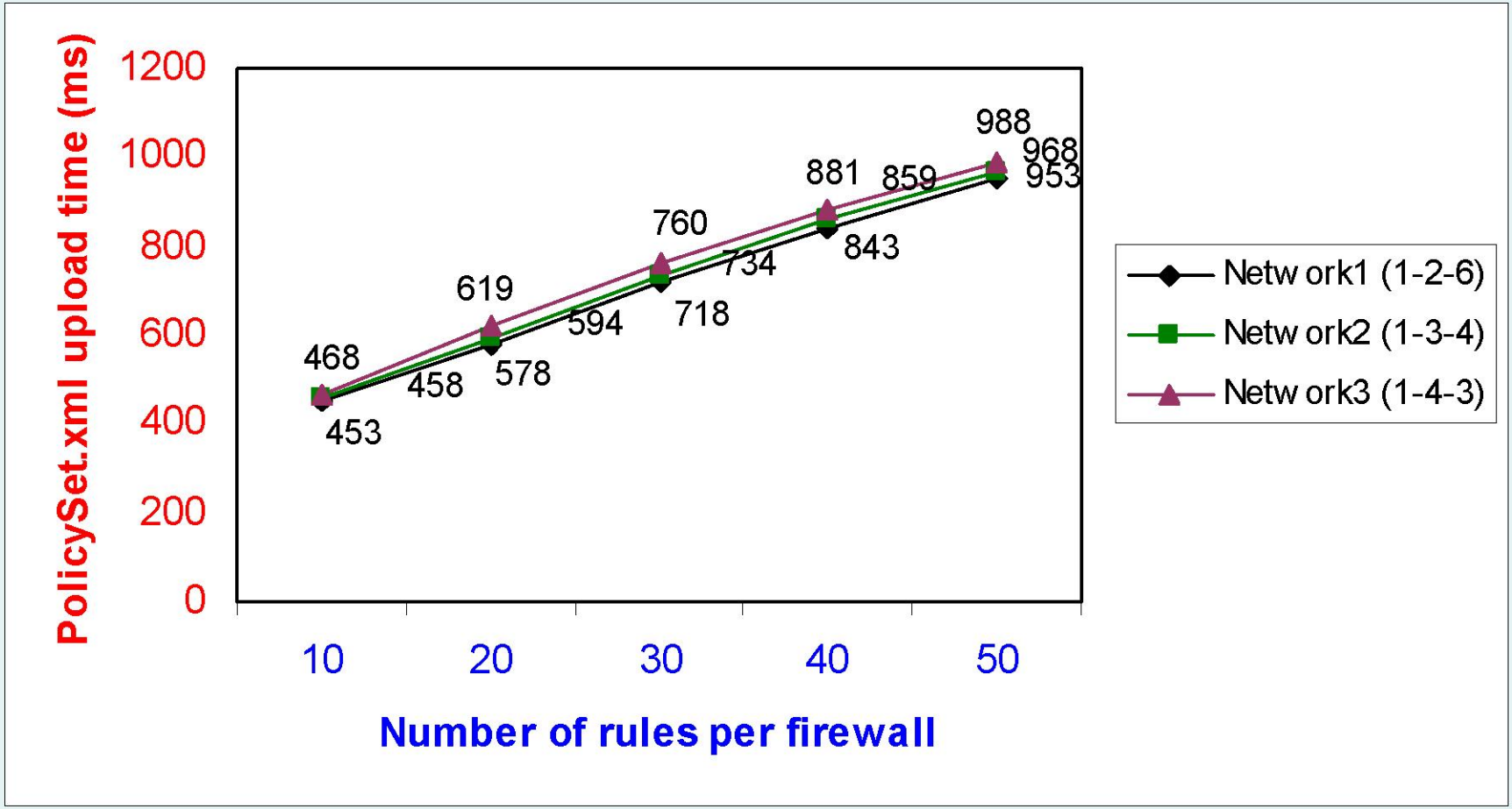
Operational Values - 2



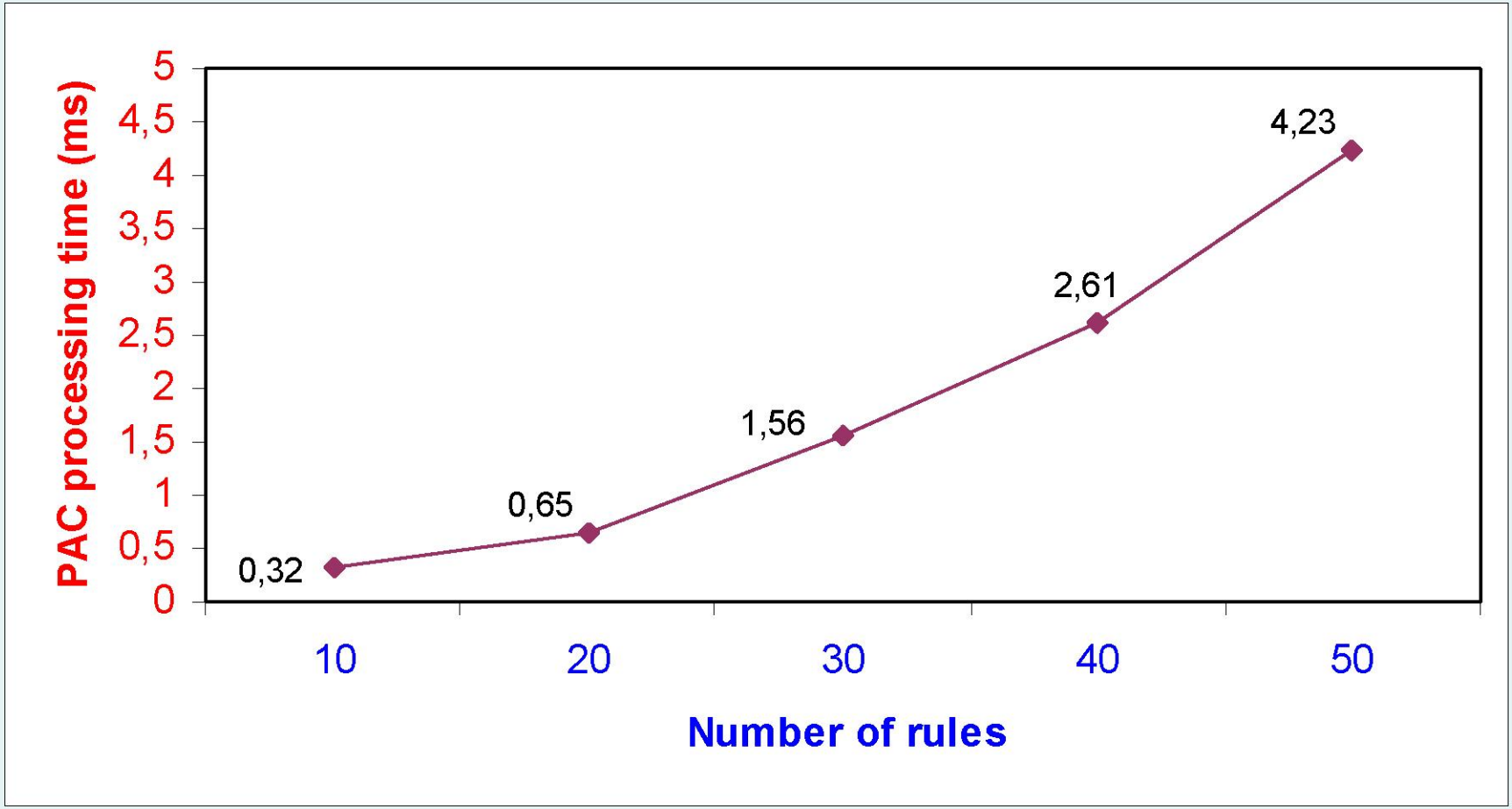
Operational Values - 3



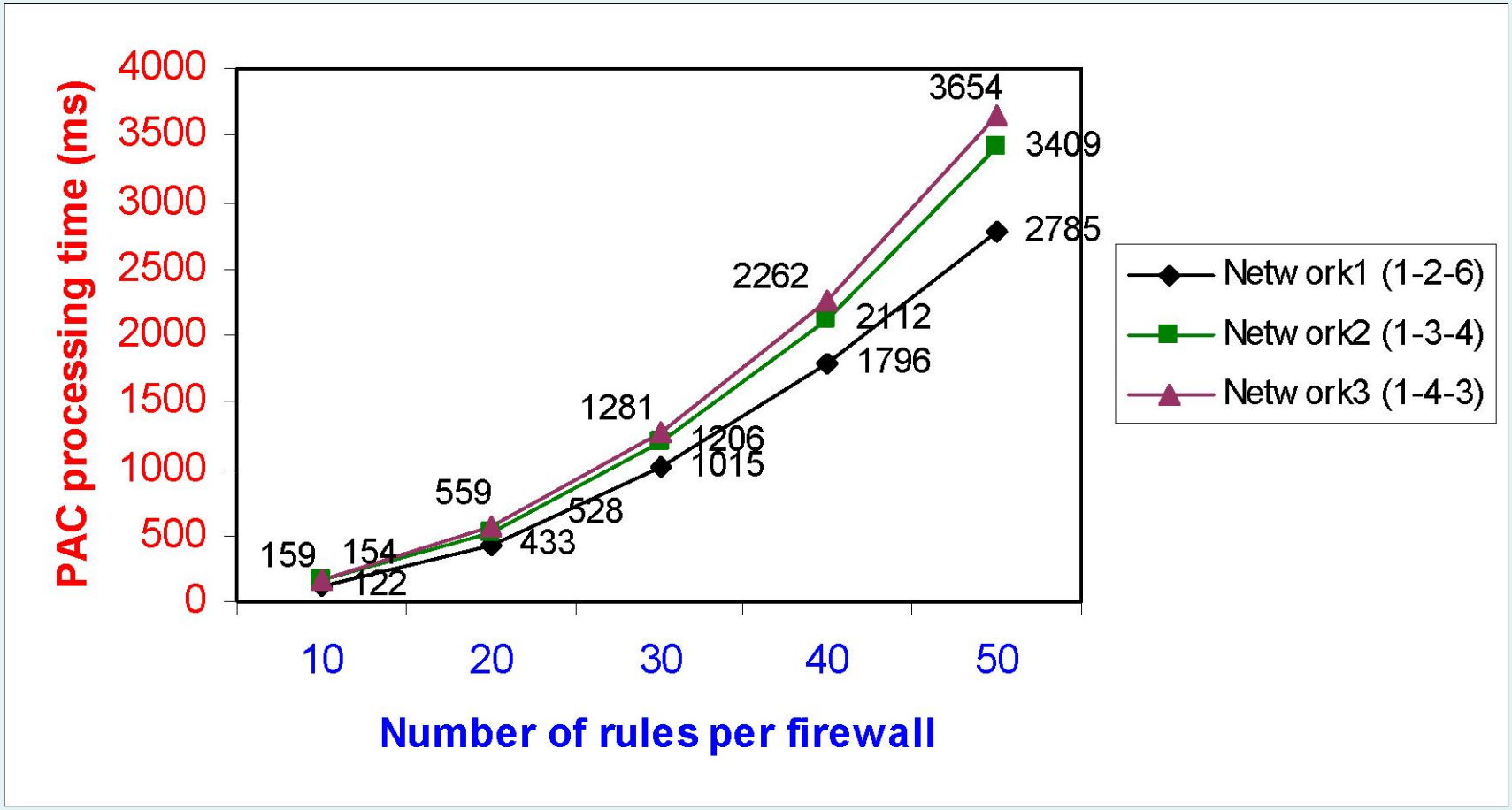
Operational Values - 4



Operational Values - 5



Operational Values - 6



Contributions

- Firewall configuration management architecture – DPS and FAs
- Firewall policy representation in XACML
- Configuration message communication
- Automatic deployment of organizational policies
- Policy anomaly checking

Future Work

- Extend our architecture so that management of a number of domains distributed over globe is possible
- Change tree based network model to graph based model
- Use SAML for communication
- Integrate a policy query manager
- Design firewall agents to be more intelligent

Thank you for your interest.

Tugkan TUGLULAR

Thank you…

Tugkan TUGLULAR

DTD for Network Topology

```
<?XML version=”1.0”?>
<!DOCTYPE Topology [
    <!ELEMENT Topology (Subnet)*>
    <!ELEMENT Subnet (Firewall)*>
    <!ATTLIST Subnet Description CDATA #REQUIRED >
    <!ELEMENT Firewall>
    <!ATTLIST Firewall Type (DFW | SFW | PFW)
            #REQUIRED IP-Address CDATA #REQUIRED >
]>
```