Policy Object for I2NSF

https://datatracker.ietf.org/doc/draft-xia-i2nsf-security-policy-object/

Liang Xia

Qiushi Lin

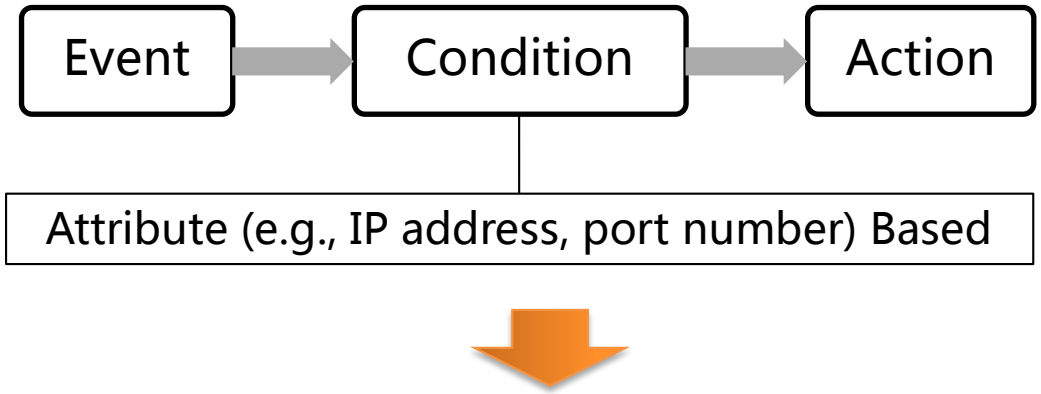
IETF 99

Background

- **Attribute Based Policy Rules – Possible Problems**

- Creation: Repetitive configuration

- Maintenance: Tedious & Time-consuming



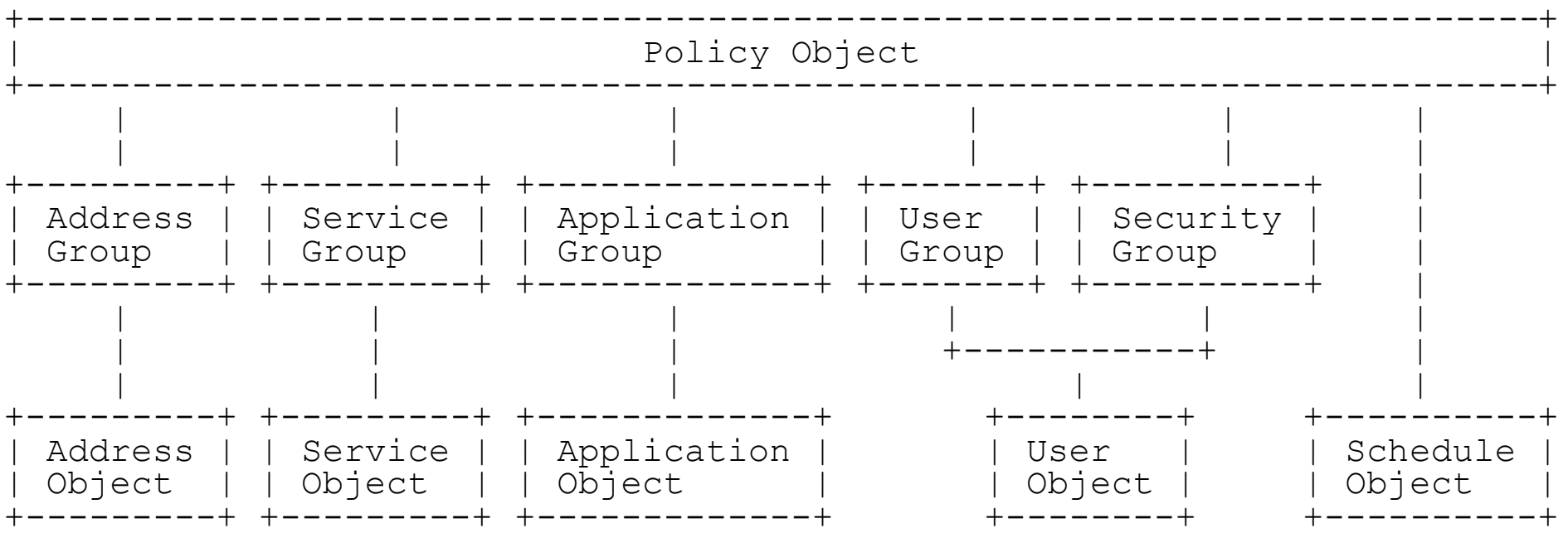
- **Object Based Policy Rules – Benefits**

- **Creation: Re-usability**

- **Maintenance: Simplicity**

Updates of Version 01

- **Provide a minimal set of policy objects and attributes**



- **Add examples**

- Possible attribute values of policy objects

- Application scenario of policy objects

Policy Object Details

Address Object

```
|
+---addressName
|
+---addressRange
```

- IPv4 address range:

Wild mask: 10.10.1.2\0.0.0.255
Subnet mask: 10.10.1.2/255.255.255.0
or 10.10.1.2/32
Start and end address: 10.0.0.50 – 10.0.0.60

- IPv6 address range:

Prefix length: a234::120/120
Start and end address: a231::a237-b231::b237

Address Group Object

```
|
+---addressGroupName
|
+---addressReference
|
+---addressRange
```

refers to existing address objects and address group objects

Policy Object Details

Service object

```
|
+---serviceName
|
+---serviceList
    |
    +---serviceProtocol            IP, ICMP, ICMPv6, TCP, UDP or SCTP
    |
    +---serviceProtocolNumber      for IP based service
    |
    +---serviceICMPType
    |                              } for ICMP or ICMPv6 based service
    +---serviceICMPCode
    |
    +---serviceSourcePort
    |                              } for TCP, UDP or SCTP based service
    +---serviceDestinationPort
```

Service Group Object

```
|
+---serviceGroupName
|
+---serviceReference
```

Policy Object Details

Application Object

```
|
+---applicationName
|
+---applicationCategory
|
+---applicationSubCategory
|
+---applicationTransmissionModel
|    (Client/Server,
|     Browser-Based,
|     Network Protocol,
|     Peer-to0Peer)
|
+---applicationVulnerability
|    (Exploitable,
|     Evasive,
|     Data Loss,
|     Used by Malware,
|     Bandwidth Consuming)
|
+---applicationRiskLevel
     e.g., 5 risk levels
```

Category	Subcategory	Example
General	General_TCP	TCP-based
	General_UDP	UDP-based
	Other	Error_Packet
Network	IP_Protocol	OSPF
	Encrypted_Tunnel	GRE, IKEv2
	Infrastructure	FTP, DNS
	...	...
General Internet	Search_Engine	Google
	Utility	Google Earth
	Web_Browsing	OperaMobile
	...	...
Entertainment	Social_Networking	Facebook
	Instant_Messaging	QQ, MSN
	Game	QQGame
	...	...
Business Systems	Internet_Conference	NetMeeting
	Email	GMail
	Database	Oracle
	...	...

Policy Object Details

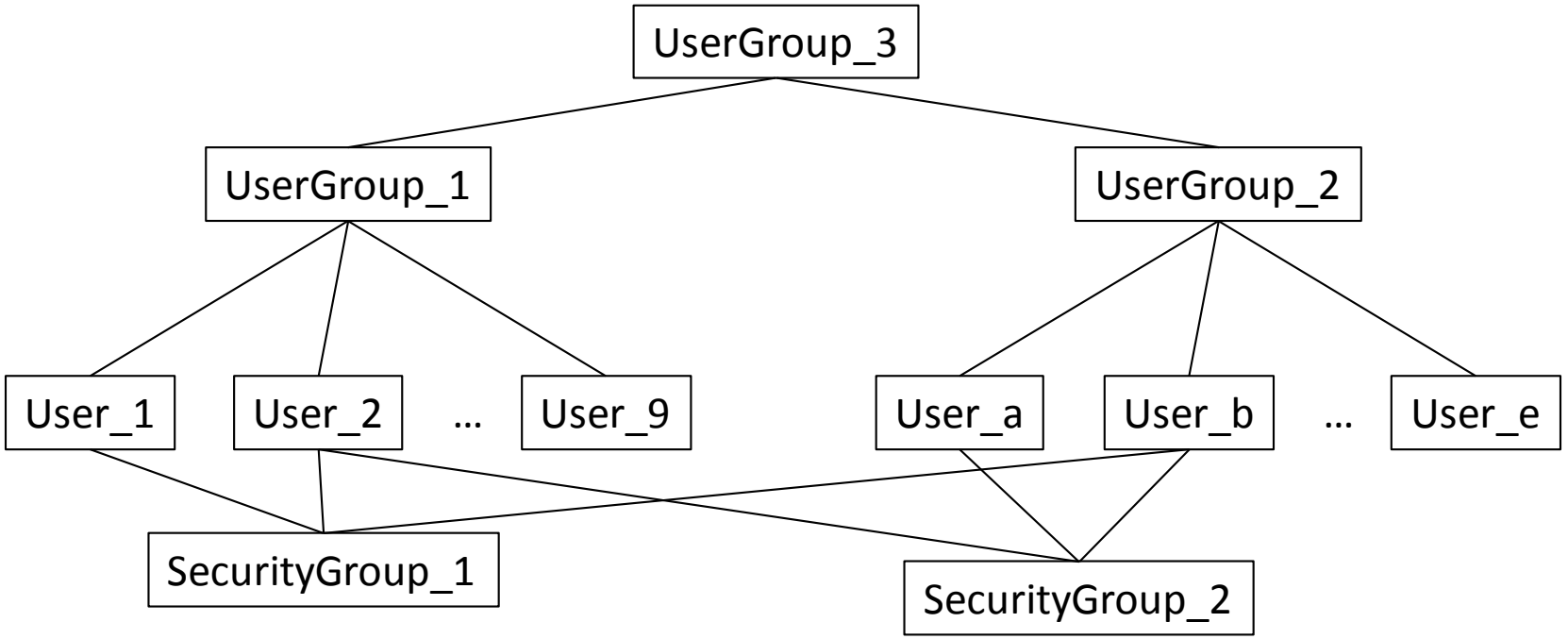
Application Group Object

```
|
+---applicationGroupName
|
+---applicationReference
```

Schedule Object

```
|
+---scheduleName
|
+---scheduleList
    |
    +---scheduleType          e.g., periodic or absolute time range
    |
    +---scheduleStartTime     periodic: start time
    |                         absolute: start time and date
    +---scheduleEndTime       periodic: end time
    |                         absolute: end time and date
    +---scheduleWeekDay       the days in a week that the periodic
                              time range takes effect
```

Policy Object Details



User Object	A person who may access network resources
User Group Object	Organized as a hierarchical structure
Security Group Object	Consist of user objects from different user group objects that require the same policy enforcement

Policy Object Details

User Object

- userName
- userParentGroup
- userSecurityGroup
- userDomain
- userPassword
- userExpirationTime

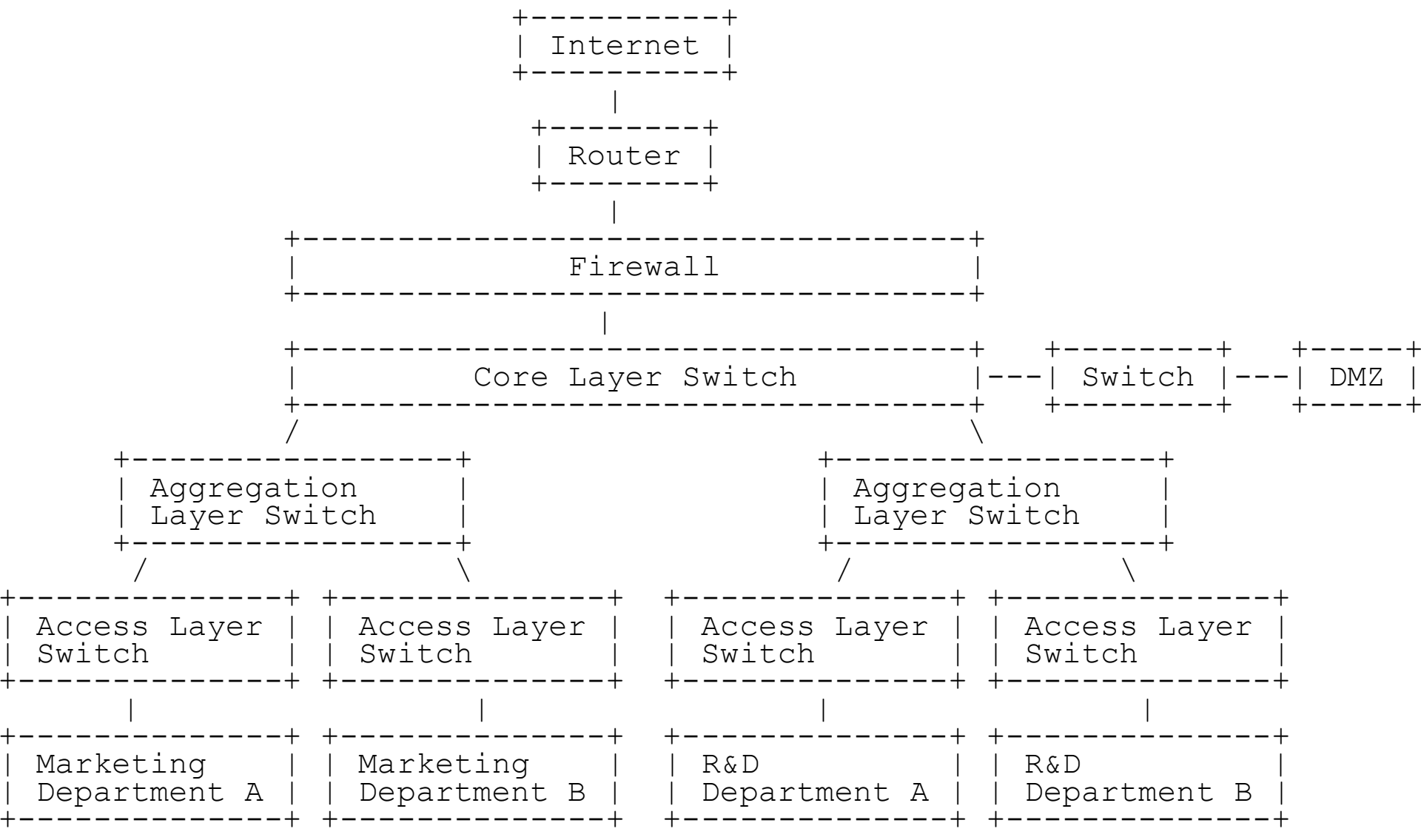
User Group Object

- userGroupName
- userGroupParentGroup
- userGroupDomain
- userGroupReference

Security Group Object

- securityGroupName
- securityGroupParentGroup
- securityGroupDomain
- securityGroupType — e.g., Static or Dynamic
- securityGroupReference
- securityGroupFilters

Example


Internet
Router
Firewall
Core Layer Switch
Switch
DMZ
Aggregation Layer Switch
Aggregation Layer Switch
Access Layer Switch
Access Layer Switch
Access Layer Switch
Access Layer Switch
Marketing Department A
Marketing Department B
R&D Department A
R&D Department B

Example

- **Security Policy Control for Marketing Departments**

Policy Objects used in Condition	Action
User Group: Marketing_A, Marketing_B Application Group: Entertainment_App Schedule: Work_Day	Deny
User Group: Marketing_A, Marketing_B Service: Web_Service	Permit

- **Security Policy Control for R&D Departments**

Policy Objects used in Condition	Action
Security Group: R&D_Manager	Permit
User Group: R&D_A, R&D_B	Deny

- **Security Policy Control for Server Access of Internet Users**

Policy Objects used in Condition	Action
Address: Server_Address	Permit

Questions/Comments

- For Event-Condition-Action model, do Event and Action also need Objects?
- Does Client-facing Interface IM need Objects?
- Is it ok to have an individual draft for Objects specification?
- Object hierarchy design? A general and original object; object inheritance and extension;
- …