Policy Object for I2NSF

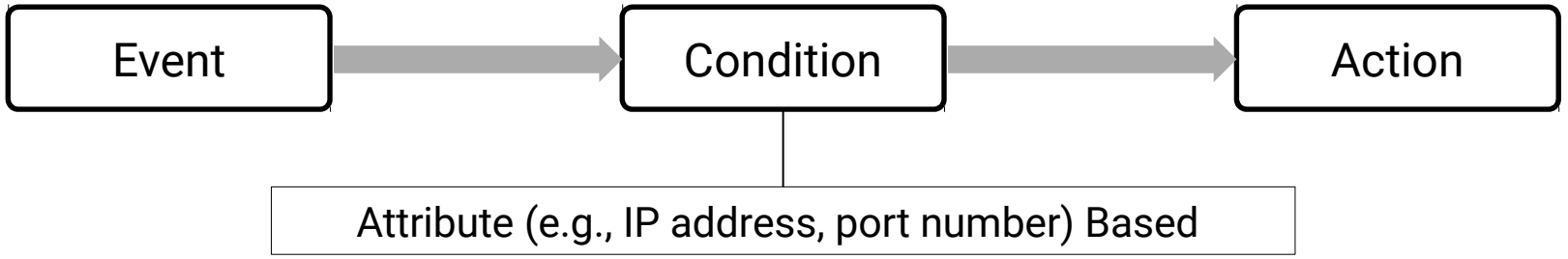
https://datatracker.ietf.org/doc/draft-xia-i2nsf-security-policy-object/

Liang Xia

Qiushi Lin

IETF 98

I2NSF Policy Rule Without Objects



Possible problems:

- Creation:
  - Repetitive configuration
- Maintenance:
  - Tedious
  - Time-consuming

Policy Object Definition

Policy objects are collections of commonly used condition attributes:

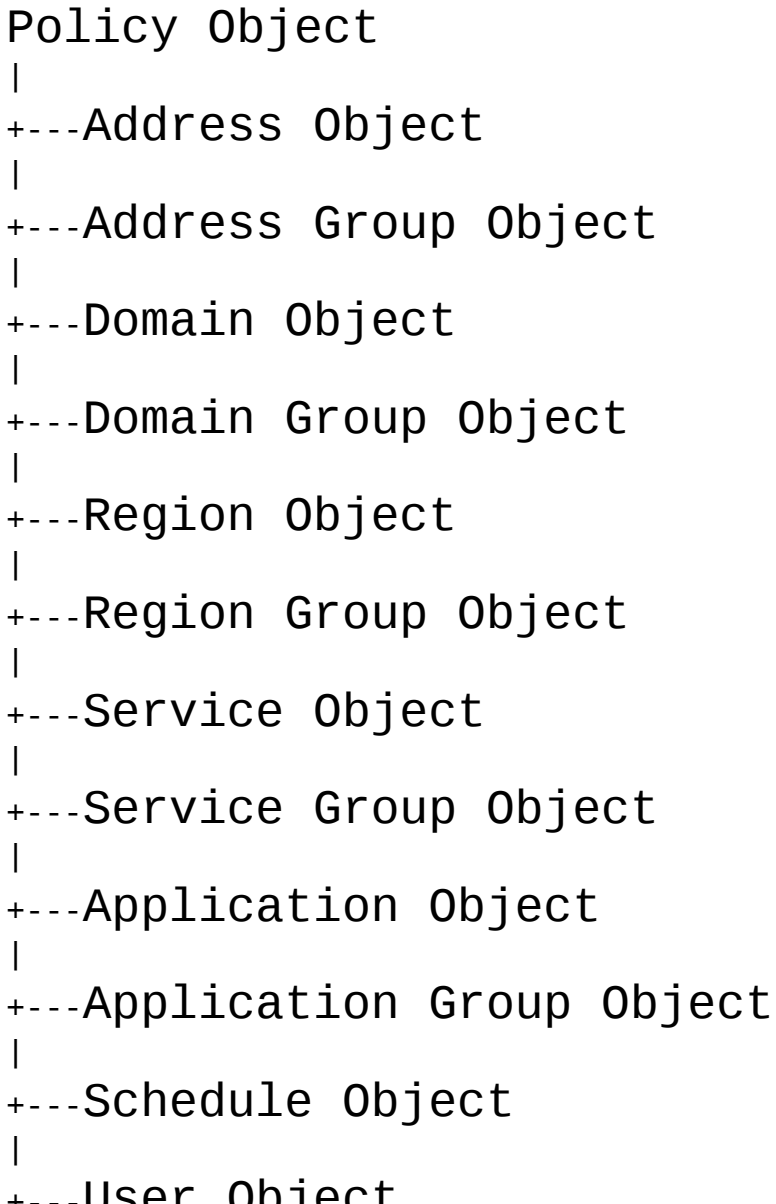
- IP address,
- Protocol type,
- TCP/UDP port number,
- Time range,
- User account,
- … …

o **Predefined and can be referenced by their unique names.**

o **Re-usability**: A policy object can be referenced in different policy rules as required.

o **Simplicity**: The modification of a policy object will be propagated to the I2NSF policy rules that reference this object.

Policy Object Overview



Policy Object Details

Address Object
|
+---addressName
|
+---addressRange e.g., 10.0.0.50 – 10.0.0.60
                  10.10.1.2/255.255.255.0
                  a234::120/120
                  ...

Address Group Object
|
+---addressGroupName
|
+---addressReference refers to existing address objects
| and address group objects
+---addressRange

Policy Object Details

Domain Object

```
|
+---domainName
|
+---domainList
```

e.g., www.example.com
*.example.com

Region Object

```
|
+---regionName
|
+---regionLocation
|   |
|   +---regionLongitude
|   |
|   +---regionLatitude
|
+---regionIPAddress
```

Domain Group Object

```
|
+---domainGroupName
|
+---domainGroupReference
|
+---domainList
```

Region Group Object

```
|
+---regionGroupName
|
+---regionGroupReference
```

Policy Object Details

```
Service object
|
+---serviceName
|
+---serviceList
    |
    +---serviceProtocol           TCP, UDP, SCTP, ICMP, ICMPv6 or IP

    |
    +---serviceProtocolNumber     for IP protocol
    |
    +---serviceSourcePort         for TCP, UDP or SCTP protocol
    |
    +---serviceDestinationPort    for TCP, UDP or SCTP protocol
    |
    +---serviceICMPType           for ICMP or ICMPv6 protocol
Service Group Object
|
+---serviceGroupName
|
+---serviceReference
```

Policy Object Details

Application Object

```
|
+---applicationName
|
+---applicationCategory              e.g., general, network application
|
+---applicationSubCategory     e.g., search engine, electronic commerce
|
+---applicationTransmissionModel     e.g., client/server, peer-to-peer
|
+---applicationLabel                        e.g., database, http-based
|
+---applicationRiskLevel                          e.g., 5 risk levels
```

Application Group Object

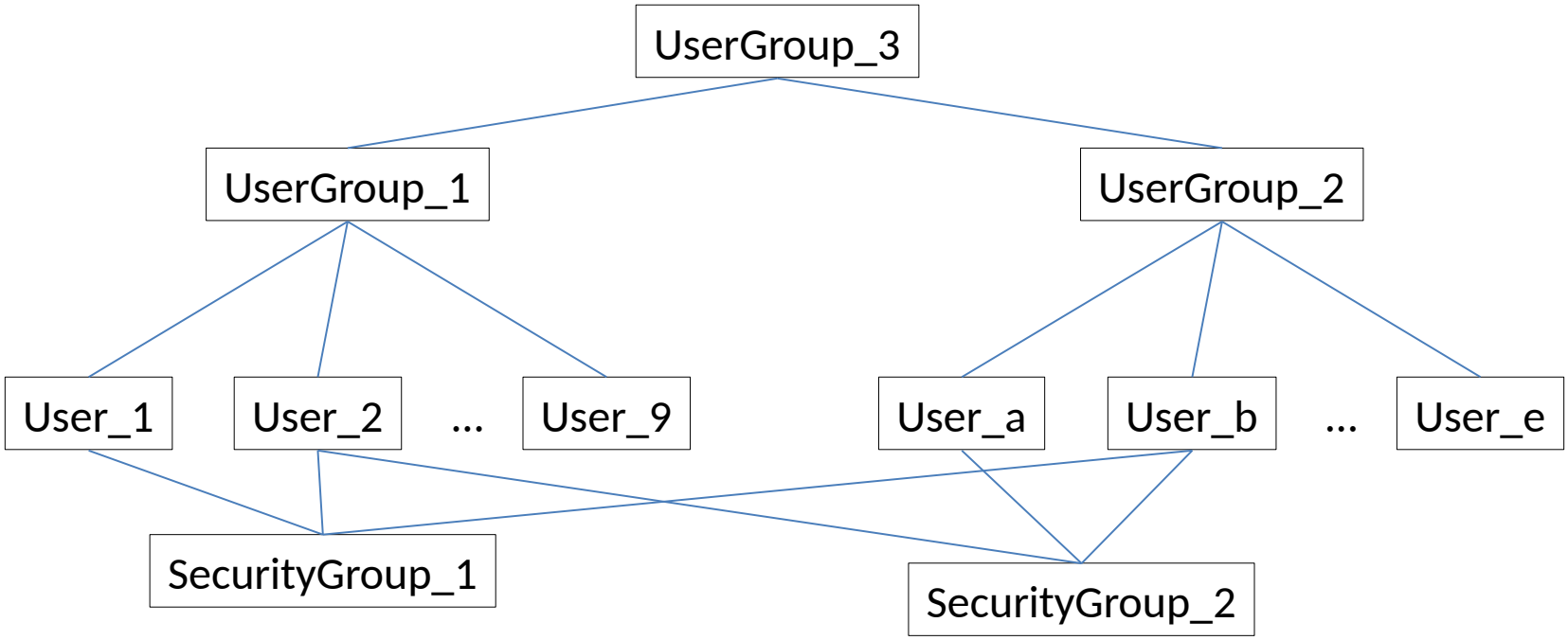
```
|
+---applicationGroupName
|
+---applicationReference
```

Policy Object Details

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



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

Policy Object

User Object

- userName
- userParentGroup
- userSecurityGroup
- userDomain
- userPassword
- userExpirationTime
- userAllowSharing
- userBindingStatus
- userBindingAddress

User Group Object

- userGroupName
- userGroupParentGroup
- userGroupDomain
- userGroupReference
- userGroupAllowSharing

Security Group Object

- securityGroupName
- securityGroupParentGroup
- securityGroupDomain
- securityGroupType
- securityGroupReference
- securityGroupFilters
- securityGroupAllowSharing

Discussion

- **Comments? Questions?**
  - ✓ 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; ...
- **Please review and comment**