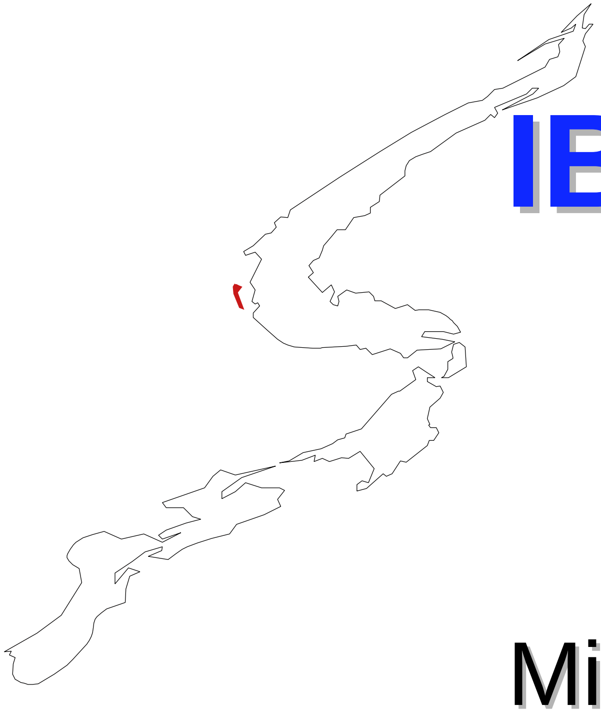
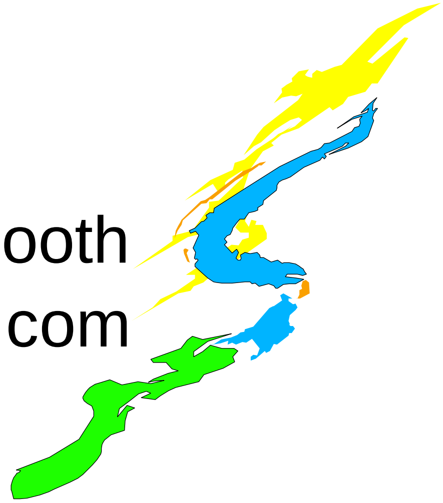


IBM's Implementation of IPSEC Policy Schema

Minneapolis IETF Meeting (March 1999)



Skip Booth
sbooth@us.ibm.com

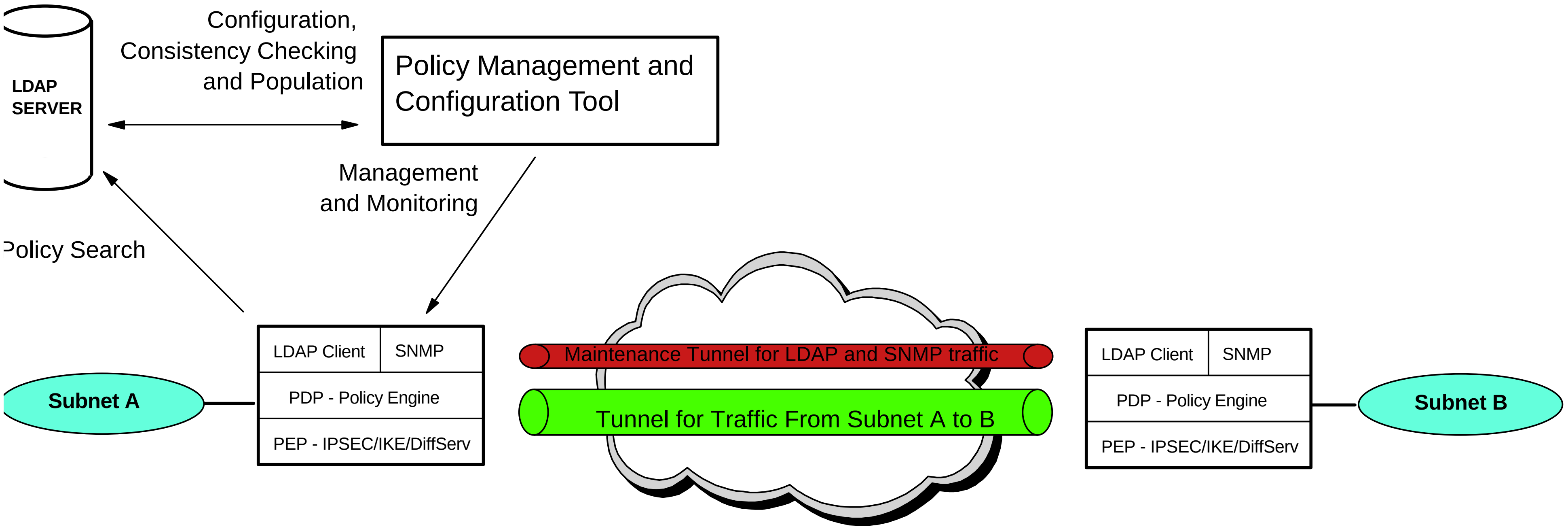
Give credit where credit is due

- draft-ipsec-vpn-policy-schema-00.txt
  - An LDAP Schema for Configuration and Administration of IPSec based Virtual Private Networks (VPNs)
    - Partha Bhattacharya, Cisco
    - Rob Adams, Cisco
    - William Dixon, Microsoft
    - Roy Pereira, Timestep
    - Raju Rajan, IBM

Objectives

- Overview of Architecture
- Differences between Implemented Schema and Draft Schema
- Issues and Recommendations

Overview of Architecture - IBM 221x Router Family



LDAP SERVER

Configuration, Consistency Checking and Population

Policy Management and Configuration Tool

Management and Monitoring

Policy Search

LDAP Client	SNMP
PDP - Policy Engine	
PEP - IPSEC/IKE/DiffServ	

Maintenance Tunnel for LDAP and SNMP traffic

Tunnel for Traffic From Subnet A to B

LDAP Client	SNMP
PDP - Policy Engine	
PEP - IPSEC/IKE/DiffServ	

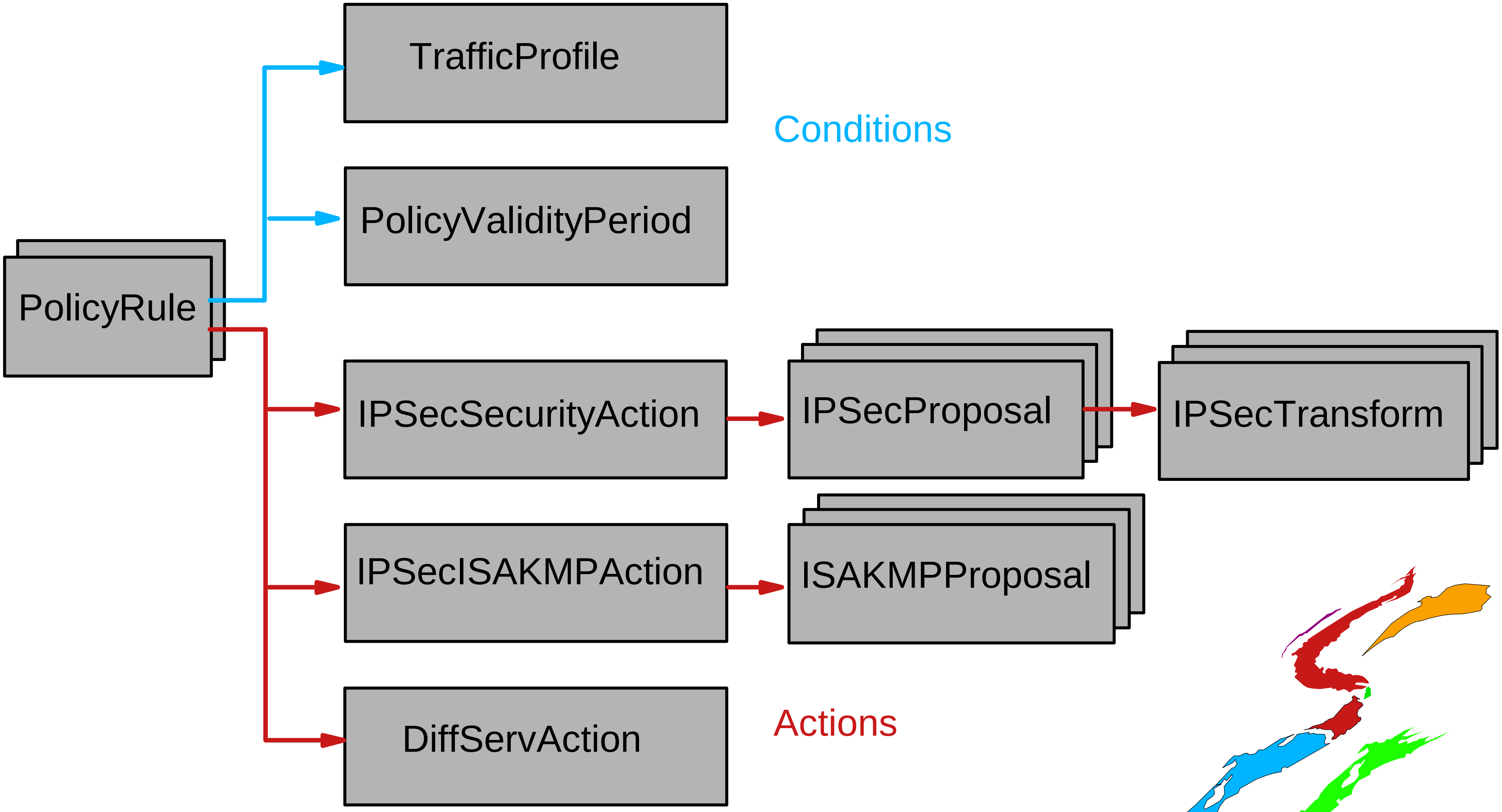
Subnet A

Subnet B

Key Points

- Integrated PDP and PEP
- Maintenance Tunnel For Management and Configuration
- Tool for Configuration, Management and Consistency Checking

IPSEC Class Relationship - IBM NHD implementation



PolicyRule

TrafficProfile

PolicyValidityPeriod

Conditions

IPSecSecurityAction

IPSecProposal

IPSecTransform

IPSecISAKMPAction

ISAKMPProposal

DiffServAction

Actions

IPSecSecurityAction Class

Definition

- Specifies the security needed for the policy:
  - drop, pass or secure with IPSEC
- If type is Secure, then the Phase2 IPSecProposals suite to negotiate must be specified

Additional Attributes Added

- **Tunnel In Tunnel** - optimization to help in "filter rule" generation
- **CopyDFBit** - In tunnel mode, specifies whether to copy/set/clear the Don't Fragment bit from original IP Header into the new outer header
- **ReplayProtection** - replay protection enabled/disabled
- **MinSARefreshPercentage** - defines the acceptable range of lifetime/sizes for all transforms in the proposal suite. (Valid range = xform lifesize/time * minSARefreshPercentage/100 to transform lifesize/time

Attributes Not Implemented

- **Connection Lifetime and LifeSize** - phase2 SA will always continue to refresh in our implementation
- **Local and Remote Proxy** - use information in the TrafficProfile as the proxy
- **ProxiedHostScope** - used a value of 0.0.0.0 for the tunnel endpoint to imply remote access policy
- **MinSecurityAssociationLifetimeSec, LifetimeKBytes** - replaced with the MinSARefresh Percentage
- **ISAKMPActionRef** - specified as an action in the policy definition

IPSecProposal Class

Definition

- Specifies the IPSecTransforms (List of AH and/or ESP and/or IPComp Transforms) to negotiate for this phase 2 proposal.
- Specifies whether PFS is needed and if so which Diffie Hellman Group to use.

Additional Attributes Added

- No attributes added

Attributes Not Implemented

- **PrivateDiffieHellmanGroupRef** - our implementation supports only DH Group 1 and Group 2

Suggestion

- Move PFS and Diffie Hellman attributes to the IPSecSecurityAction since all proposals during the phase2 negotiation must have the same DH group.

IPSecTransform Class

Definition

- Specifies the authentication and/or encryption parameters for IPSEC or the compression parameters for IPComp.
- Specifies the lifetime and lifesize for the transform
- For ESP or AH, specifies the encapsulation mode

Additional Attributes Added

- No attributes added

Attributes Not Implemented

- **ESPCipherKeyLength, ESPCipherKeyRounds** - our supported encryption algorithms do not require these attributes to be defined
- **Compression Attributes** - IP Compression not currently supported

Suggestion

- Make lifesize and lifetime values a range and remove the MinSARefreshPercentage attribute from the IPSecSecurityAction

IPSecISAKMPAction Class

Definition

- Specifies the phase 1 attributes and proposals to negotiate during phase 1

Additional Attributes Added

- **minSARefreshPercentage** - defines the acceptable range of lifetime/sizes for all the proposals in the phase 1 suite. (Valid range = proposal lifesize/time * minSARefreshPercentage/100 to proposal lifesize/time

Attributes Not Implemented

- **LocalHostPublicKeyInfo, RemoteHostPublicKeyInfo** - current implementation does not allow this flexibility
- **MinSecurityAssociationLifetimeSec, KBytes** - replaced these two attributes with the minSARefreshPercentage
- **SecurityAssociationRefreshThreshold** - our implementation does not automatically refresh the phase 1 SA

Suggestion

- Move the Public Key Information into a separate object to make the IPSecISAKMPAction more reusable

ISAKMPProposal Class

Definition

- Specifies the security and identification algorithms to use as well as the authentication method to use.
- Specifies the lifetime/size to negotiate and enforce for this proposal

Additional Attributes Added

- No attributes added

Attributes Not Implemented

- **ISAKMPPrfAlgorithm**
- **ISAKMPCipherKeyLength, ISAKMPCipherKeyRounds** - Supported Encryption algorithms do not require these attributes
- **PrivateDiffieHellmanGroupRef** - only support DH Group 1 and Group 2

Suggestion

- Make the lifetime and lifesize a range and remove the minSARefreshPercentage from the IPSecISAKMPAction

Issue 1

- How to handle Policies with Condition Lists of the form DNF/CNF and negation. This specifically becomes a problem when the Proxy and IPSEC tunnel endpoints must be specified in the IPSecSecurityAction

Issue 1 (cont.) CNF example

Problem:

- One policy can define multiple tunnels
- Each tunnel has different proxies
- Each tunnel is potentially protected by different security gateways
- Logically only one IPSecSecurityAction should be associated with the Policy

Example(CNF):

- if ((Traffic originated from Subnet 10.2.0.0 to 12.2.0.0) OR (Traffic originated from Subnet 11.1.0.0 to Subnet 12.1.0.0)) AND (time is during 9 to 5, Mon through Friday)

Options:

- Limit the Condition in the policy to a singular expression
- ★ Remove Proxy information and Tunnel information from IPSecSecurityAction and use the information in the IPPolicyCondition to determine the proxy
- Each Condition Must make a reference to an Action

Issue 2

- Semantics of a Security Policy - is there one policy that specifies the entire information for the security or are there multiple "filter rules" that together specify the security policy for traffic

Issue 2 (cont.)

- Current schema was envisioned to produce the following PolicyRule:
  - Example: Traffic From A to B, tunnel endpoints SG1 and SG2, protect with IPSEC (SG1's perspective):
    - 1) Condition: Traffic From A to B
      - Action: IPSecSecurityAction (type = pass with security)
    - 2) Condition: Traffic From B to A
      - Action: IPSecSecurityAction (type = Permit if Packet arrived in Tunnel)
    - 3) Condition: IPSEC Traffic from SG1 to SG2
      - Action: IPSecSecurityAction (type = pass with no security)
    - 4) Condition: IKE Phase 2 Traffic from SG2 to SG1
      - Action: IPSecSecurityAction (negotiate phase 2 proposal suite)
    - 5) Condition: IKE Phase 1 Traffic from SG1 to SG2
      - Action: IPSecISAKMPAction (negotiate phase 1 proposal suite)
    - 6) Condition: IKE Phase 1 Traffic from SG2 to SG1
      - Action: IPSecISAKMPAction (negotiate phase 1 proposal suite)
- IBM NHD implementation only requires one policy to be entered in the directory for SG1
  - Policy entered is essentially the "Traffic Condition" with the IPSecSecurityAction and the IPSecISAKMPAction specified in the policy definition (rule 1 above)
  - "Filter Rules" are generated by the Policy Decision Point

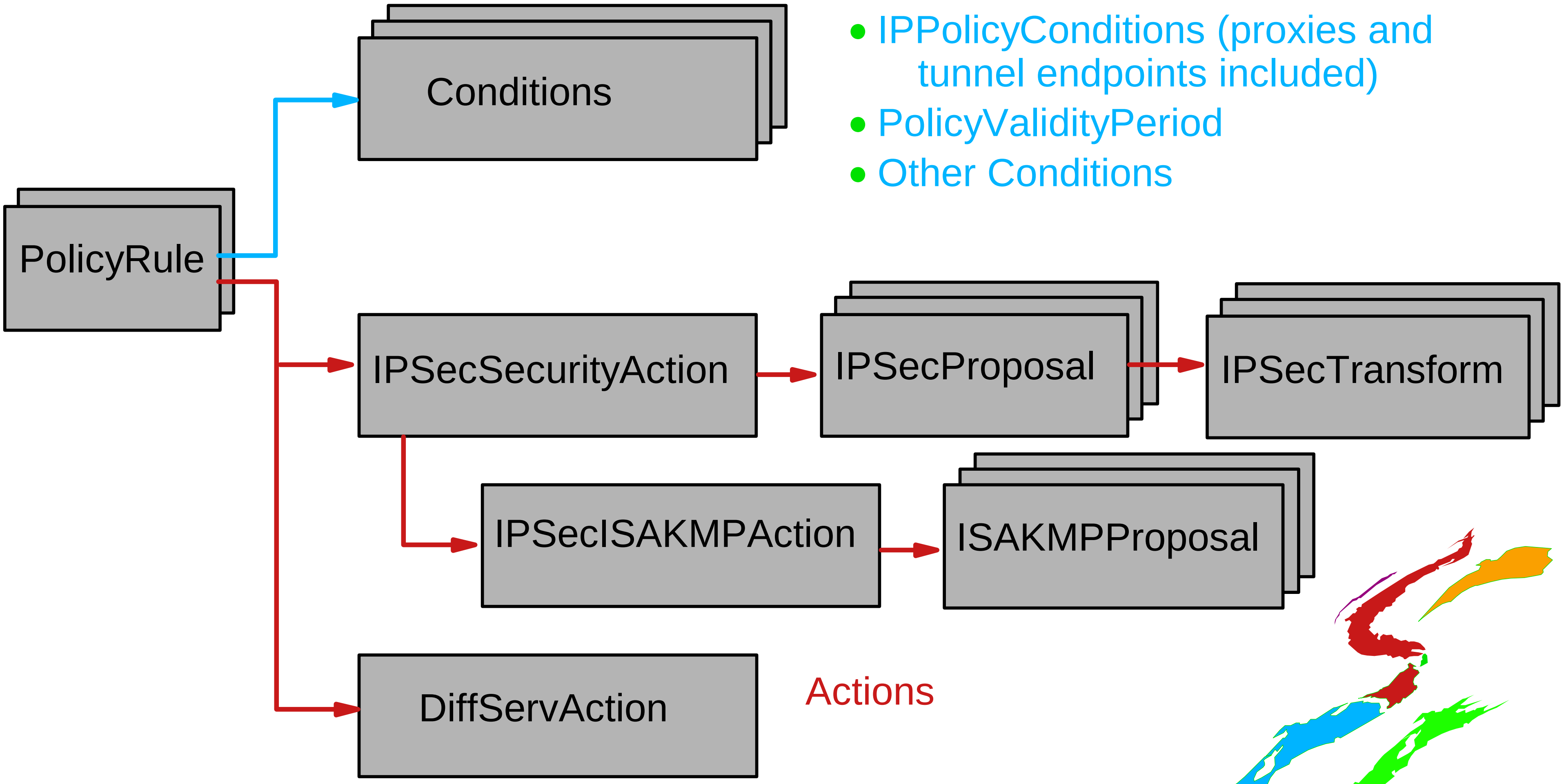
Issue 3

- In a heterogeneous environment, how does the management tool determine the correct level of security when devices do not support the same level of functionality
  - Export limitations may cause some devices to only support DES whereas others support DES and 3DES
  - Devices from different venders supporting different sets of encryption and integrity algorithms as well as different authentication methods
- Recommendation
  - Define a VPN Capabilities MIB that allows the management station to interrogate the hosts and gateways in the network to determine how to define and resolve the correct level of security policy information

Recommendation

- Submit an informational draft that defines "standard" templates for the VPN Security Classes defined in the VPN schema.
    - Using the syntax defined in "draft-ipsec-vpn-policy-schema-00.txt" define abstract terminology which maps specific settings for attributes within the each class
        - "Strong Security", "Very Strong Security", etc.
    - IF we could map abstract terms around specific instances of the schema definitions then every vendor's configuration panels could use the same terminology and hopefully reduce operational problems for our customers

Suggested IPSEC Class Relationship based on Core Policy Schema



Conditions

- IPPolicyConditions (proxies and tunnel endpoints included)
- PolicyValidityPeriod
- Other Conditions

Actions