A Policy Information Model for RFC2547-like IP VPNs

Arnaud Gonguet, Olivier Poupel
Alcatel R&I, Route de Nozay, 91460 Marcoussis, France

Abstract: This article presents a Policy Information Model for RFC2547-like IP VPNs. Policy Information Models are the key component of Policy-based Management systems. They describe a set of service specific policy conditions and/or policy actions, used to formulate the policy rules to formalise a service.

In this article, the principles of Policy-based Management are reminded and the role and usage of Policy Information Models is introduced. Then this article provides a description of the way an RFC2547-like IP VPN is provisioned in a network. Finally the authors propose a Policy Information Model for managing RFC2547-like IP VPNs.

Keywords: BGP/MPLS VPNs, Policy Information Model

1. INTRODUCTION

This article presents an IP Virtual Private Network (VPN) Policy Information Model. The targeted VPN service is based on an IP network where MPLS is used for forwarding packets over the core, and BGP is used for distributing routes over the core. Moreover, only the case of a network based (or PE-based) VPN is considered here. These kind of IP VPNs are described in RFC 2547 [1]. They will be called hereafter RFC2547-like IP VPNs. Policy information models are used in the context of Policy-based Management, which principles are defined in [2]. The IP VPN Policy Information Model presented hereafter defines a set of policy actions related to the management of RFC2547-like IP VPNs services, that will be used to implement policy rules that are the key components of Policy-based Management.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35620-4_43
D. Gaïti et al. (eds.), *Network Control and Engineering for QoS, Security and Mobility*

In the first section, this article presents the principles of Policy-based Management, and the advantages of such a network management system. The second section underlines the role and usage of the Policy Information Models in the context of Policy-based Management. The third section explains the provisioning mechanisms of an RFC2547-like IP VPN service. The last section presents a Policy Information Model for RFC2547-like IP VPNs services.

2. POLICY-BASED MANAGEMENT PRINCIPLES

The legacy network management methodologies, that aim at translating service objectives directly into network device configuration commands, are showing some restrictions [3]:

- Telnet and CLI (Command Line Interface) are dependent of the underlying platform, have a complex syntax and nearly no semantics.
- The use of SNMP (Simple Network Management Protocol) to browse network elements MIBs (Management Information Base) and PIBs (Policy Information Base) is subject to frequent errors. Moreover, the existence of private MIBs and PIBs hampers interoperability.

These restrictions have motivated standardisation bodies like the DMTF (Distributed Management Task Force) and the IETF (Internet Engineering Task Force) to lay the foundations of Policy-based Management. The idea is to describe the service objectives with network level policy rules that are automatically disseminated and translated into network device configuration commands.

Policy rules are written using an "If <Condition> then <Do Actions>" formalism. The details of the "conditions" and "actions" are described in the Policy Information Models, that define how to represent a rule, how to group elementary conditions to make a more complex condition, and the way conditions and actions are linked to the policy rule structure.

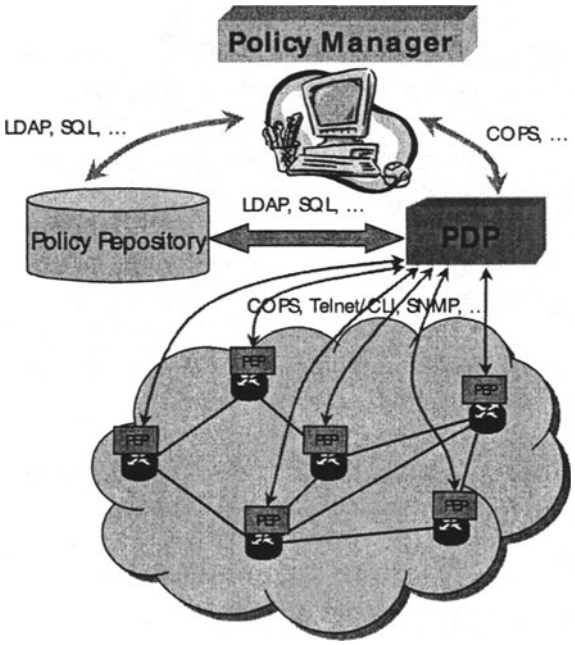

Figure 1. Architecture of Policy-based Management

The simplified architecture related to policy-based management (*Figure 1*) is made of four elements [4]:

- The Policy Manager, for editing policy rules, managing the Policy Repository, and updating new policy rules to the Policy Decision Points.
- The Policy Repository, storing the policy rules in a database.
- The Policy Decision Point (PDP), checking the coherency of the policy rules, notifying the Policy Enforcement Points of the policy rules to be applied, and taking policy decisions that are distributed to the Policy Enforcement Points.
- The Policy Enforcement Points (PEP), applying the policy rules and decisions received from the PDP and notifying the results to the PDP.

The protocols recommended by the IETF for network Policy-based Management are COPS (Common Open Policy Service) for the communications between the PDP and PEPs, and LDAP (Lightweight Directory Access Protocol) for the communication with the Policy Repository. Other protocols, like SNMP or SQL (Structured Query Language) that are widely used within the Internet can also be used for the communications between the components described above.

Policy-based Management has several advantages:

- Network management is more scalable, as adding devices to the network does not change the service level policy rules.
- Operators are liberated from the complexity of translating service objectives into network device configuration commands, as this complexity is moved to the network management.
- Network management is eased by coherency checking that can be automatically performed with regard to resources availability, configuration conflicts, or fault recovering functions.

Policy-based Management is currently mainly used for QoS provisioning, or for security management purpose. Network management can gain coherency and efficiency by using Policy-based Management for all kinds of services. To do so, the key element is to define the proper Policy Information Models to be able to model the device configuration.

3. INTRODUCTION TO THE POLICY INFORMATION MODELS

Policy Information Models are the key elements of Policy-based Management. They provide the formalism for describing a network service using policy rules. A Policy Information Model is a set of classes that enable to implement policy rules.

As explained in the previous section, the policy rules that express the service objectives are described using policy conditions and policy actions. The basic policy rules, conditions and actions are formalised in Policy Core Information Model (PCIM) [2] and its extensions PCIMe [5], as a set of PolicyRule, PolicyCondition and PolicyAction classes and a set of aggregation definitions. PCIM and PCIMe, defined at the IETF, themselves derive from the Common Information Model (CIM) [6] from the DMTF. More specific policy conditions and actions can be defined in other Policy Information Models, as the Policy QoS Information Model (QPIM) [7] from the IETF. They will be formalised as classes that inherit from the PCIMe PolicyAction or PolicyCondition classes. The RFC2547-like IP VPN Policy Information Model, defined in this article, is such an example, in which policy actions that are specific to RFC2547-like IP VPN provisioning are defined on top of the PCIMe legacy classes.

Some information is added to the service objectives when they are translated into policy rules. A service objective is a high level view of a service, that makes an abstraction of the network complexity. For example it

can describe that a VPN is needed between two given sites. The routers that will be involved are not known at this level. The policy rules that will describe this service will mention the interfaces to connect together, as well as the VPN routes distribution behaviour. Thus the mapping from service objectives to policy rules is not direct, but adds complexity.

The mapping from service objectives to policy rules is done by a functional block of service/network management, that has knowledge of both service objectives and network management data.

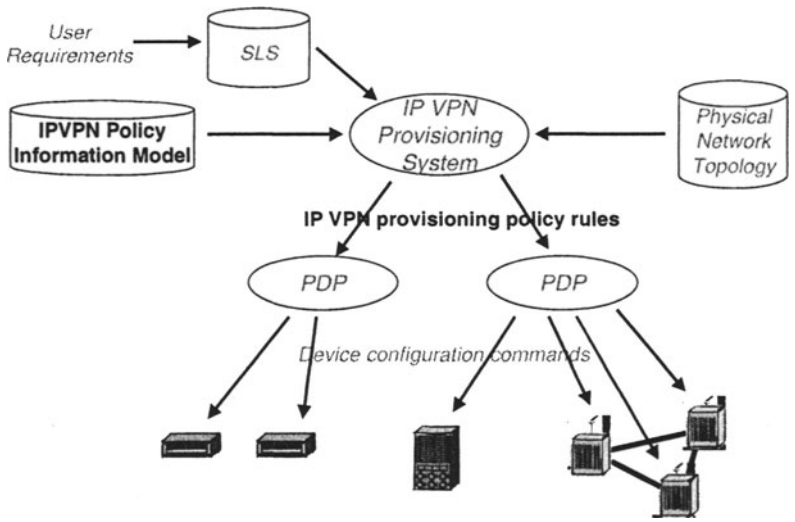

Figure 2. Usage of the Policy Information Model

In the example of *Figure 2*, the IP VPN service objectives are captured within an SLS (Service Level Specification). The IP VPN provisioning system will map those objectives into IP VPN provisioning policy rules. For that purpose it uses both the IP VPN Policy Information Model and some network management data. The Policy Information Model provides the policy rules formalism, while the network management data provides the necessary information for filling the policy condition and action parameters.

The IP VPN provisioning system is the Policy Manager defined in the previous section (*Figure 1*). After the mapping, Policy rules will be transferred to PDPs. The PDPs will translate the policy rules into device specific configuration commands. The network equipments are configured using COPS-PR, specifically defined for policy rules provisioning on NEs.

The way an SLS is converted into policy rules and policy rules are converted into routers configuration instructions is described in [8].

4. THE RFC2547-LIKE IP VPN PRINCIPLES

Provisioning an RFC2547-like IP VPN requires first to set up the IP VPN membership configuration. That means to provision routers with VPN membership information. Then it is required to set up the IP VPN connectivity, that is to manage the route distribution between the VPN routers. It is finally possible to provision the VPN routers with some firewall, NAT or encryption information, to set up some particular behaviors of the VPN.

4.1 Setting up the IP VPN membership configuration

RFC 2547 [1] defines a way to implement large scale IP VPNs. Severe scalability problems will occur if each router in the core has to maintain routing information for all the VPNs. It is important therefore that the routing information about a particular VPN is only required to be present in edge routers (i.e. PE) related to that VPN. Therefore an RFC2547-like IP VPN is implemented by managing only the PEs. The security and the confidentiality of the transported packets are supposed to be guaranteed by the core.

RFC2547-like IP VPN membership configuration is physically assured at the PE access interfaces. A site that belong to the VPN is connected to a PE via a given interface. This interface is associated with a separate forwarding table in the PE, known as VPN Routing and Forwarding table (VRF).

When a PE router receives a packet from a VPN site (via the appropriate CE), the interface through which the packet arrives determines the forwarding table used for processing that packet (*Figure 3*). The choice of a forwarding table is not determined by the user content of the packet.

To prevent a VPN to be accessed by a non member site, we decided that a VRF is associated with one and only one VPN, even if RFC 2547 [1] is not so restrictive. Different sites accessing the same VPN through the same PE can use the same VRF. In that case the VRF will be associated to more than one interface.

Setting up the IP VPN membership configuration consists of creating VRFs on PE routers, that are associated to the sites connection interfaces to those PEs.

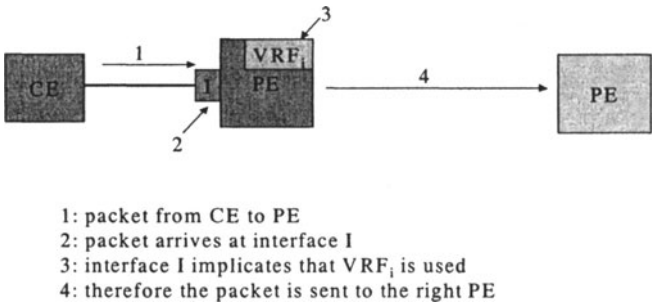

Figure 3. How the VRF is working

4.2 Setting up the IP VPN connectivity

To connect a site to a VPN via a given PE, a VRF is created on the PE and associated with the site connection interface to that PE. Then BGP automatically populates the VRF with the addresses of the site, and BGP peers are defined for this VRF. The site addresses, that may not be unique, are turned into VPN specific and unique IP addresses by adding a Route Distinguisher to the IP addresses. Those Route Distinguisher attribute and BGP peer management are performed independently from the service objectives mapping to policy rules, and are not modelled in the Policy Information Model.

The IP connectivity between the VPN sites is determined by the BGP route distribution between VRFs. Each VRF is associated with one or more "Import Route Target" attributes, and one or more "Export Route Target" attributes. BGP associates a distribution label corresponding to the VRF "Export Route Target" to the VRF routes it distributes. BGP then populates the VRFs it encounters if the encountered VRF "Import Route Target" is equal to the BGP distribution label.

In *Figure 4*, site 1 and site 2 belong to VPN A. The VPN connectivity allows site 1 to send packets to site 2, while site 2 cannot access site 1. The routes from site 2 must be distributed to the PE of site 1. The export Route Target from the PE of site 2 and the import Route Target from the PE of site 1 are set to A.

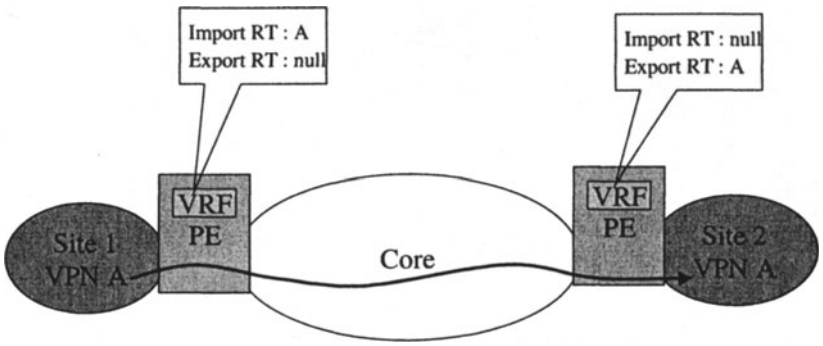

Figure 4. VRF Route Target management example

Setting up the IP VPN connectivity consists of providing the VRFs with coherent export and import Route Target attributes, so that BGP can properly distribute the routes.

5. AN RFC2547-LIKE IP VPN POLICY INFORMATION MODEL

5.1 IP VPN topology Model description

The IP VPN topology model defined hereafter aims at providing a way to visualise the VPN service to be provisioned, in order to help its modelization using policy rules. When a policy rule refers to a topology element, the derived device configuration commands will refer to a logical network representation of this element. This does not mean that a reference is made to an object instantiation of this element: the way the IP VPN topology model could be used for policy management purpose is outside of the scope of this article.

The topology information model of the IP VPN (*Figure 5*) includes a description of the physical network that will support the service and a description of the logical topology of the IP VPN. The physical network is only composed of edge nodes and edge node interfaces. The IP VPN is logically defined by a set of routing tables implemented on the edge nodes and a reference to the IP VPN service.

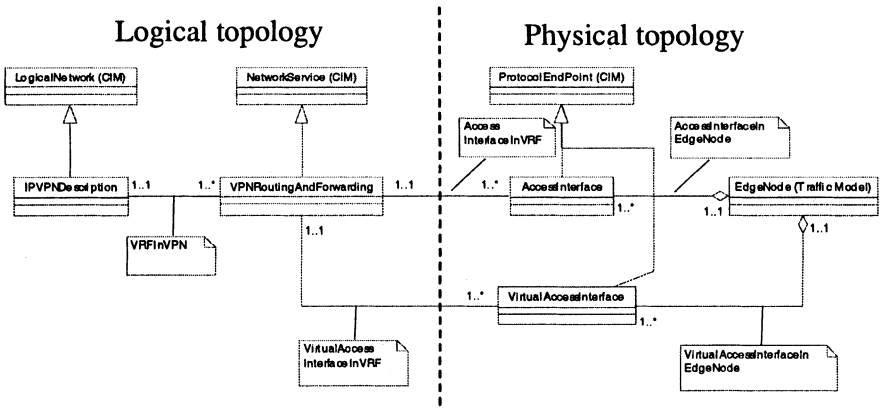

Figure 5. RFC2547-like IP VPN topology model

The physical topology of the network is described with three classes:

- The *EdgeNode* class inherits from the ProtocolEndPoint CIM class. For an RFC2547-like IP VPN it represents a PE router. It has a set of access interfaces, that can be virtual access interfaces.
- The *AccessInterface* class inherits from the ProtocolEndPoint CIM class. It represents an interface that is aggregated to an edge node. When implementing an IP VPN service, it can be associated with one, and only one, VRF table (to conform with our choice explained in the previous section).
- The *VirtualAccessInterface* class inherits from the ProtocolEndPoint CIM. It represents a sub-interface that is aggregated to an edge node. When implementing an IP VPN service, it is associated with one, and only one, VRF table.

The logical topology is described with two classes:

- The *VPNRoutingAndForwarding* class inherits from the NetworkService CIM class. It represents a PE router VRF that is associated with at least one VPN. It is associated with a set of access interfaces or virtual access interfaces of the same PE.
- The *IPVPNDescription* class inherits from the LogicalNetwork CIM. It represents the logical IP VPN. It is associated with a set of VPNRoutingAndForwarding that represents the PE routers connection to the IP VPN service.

5.2 IP VPN Provisioning Actions

The provisioning of an RFC2547-like IP VPN is done in three steps (*Figure 6*). First the membership configuration is set up by creating on the PEs, for each site connected to a PE via a given interface, a VRF associated to the interface. Then the IP connectivity is set up by configuring Route Target attributes on the VRFs to manage the BGP route distribution. Additionally some firewall, encryption or NAT behaviors can be provisioned on the PEs.

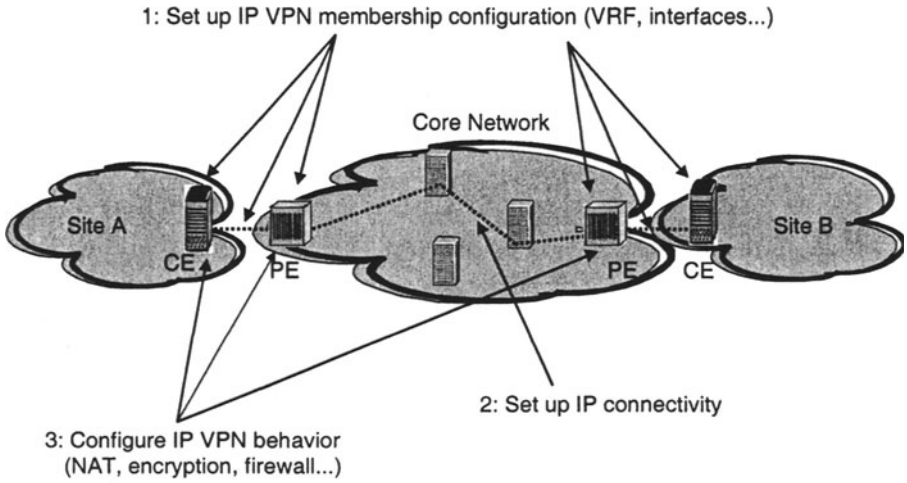

Figure 6. Provisioning of the IP VPN service

In a Policy Information Model, those actions are modelled as classes that are derived from the PCIMe PolicyAction class. Those classes are used to describe the "action" part of the policy rules that define the IP VPN service.

These actions are listed below (*Figure 7*):

- *ProvisionVRFPolicyAction* class: defines the IP VPN membership configuration. It specifies one or several PE interfaces (*attachedInterface* properties) to which sites belonging to the IP VPN are connected. When this action is processed, a VRF is created and attached to this set of interfaces.
- *ConfigureVRFPolicyAction* class: defines the IP VPN connectivity. It specifies one or several PE interfaces (*distributionSource* properties) that are connected to one or several interfaces of another PE (*distributionDestination* properties), via possible mandatory hops (*distributionMandatoryHops* properties). When this action is

processed, the routes from the VRF connected to the *distributionSource* interfaces are distributed by a BGP protocol to the VRFs connected to the distributionDestination interfaces. This is implemented through Route Target attributes mechanisms.

- *NATAction* class: defines the NAT behavior for a given PE. It specifies the set of IPv4 addresses that needs to be translated (*translateFromIPv4Address* properties) and the final set of Ipv4 addresses (*translateToIPv4Address* properties).
- *FirewallAction* class: defines the firewall behavior for a given PE (*firewallAction* property).
- *EncryptionAction* class: defines the IPSec encryption behaviour for a given PE. The set of properties required to configure the encryption is defined.

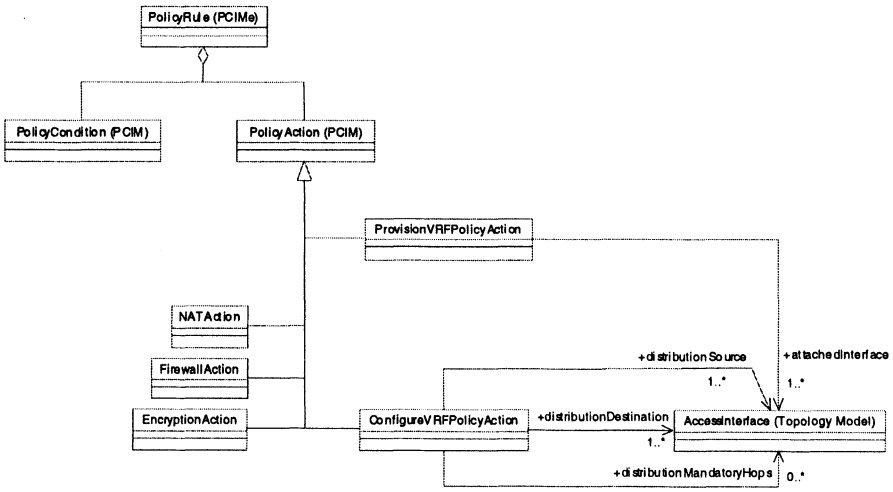

Figure 7. RFC2547-like IP VPNs Policy Information Model

6. CONCLUSION

This article presents the basis of Policy-based Management, and particularly the role and usage of Policy Information Models. A Policy Information Model is proposed for the provisioning of RFC2547-like IP VPNs. This work is proposed at the IETF [10].

Policy Information Models are a key element for Policy-based Management, and a lot of efficiency and coherency could be gained in

network management from using Policy-based Management not only for QoS or security purposes, but also for all kinds of service management.

By leading research activities in Policy-based Management, Alcatel actively contributes to develop tomorrow tools which will allow to gain efficiency and coherency to manage next generation networks.

7. REFERENCES

[1] IETF-draft, "BGP/MPLS VPNs", draft-ietf-ppvpn-rfc2547bis-01.txt, E. C. Rosen, Y. Rekhter, S. J. Brannon, C. J. Chase, J. De Clercq, P. Hitchen, D. Marshall, M. J. Morrow, A. Vedrenne, January 2002, work in progress, expire in July 2002

[2] IETF-RFC 3060, "Policy Core Information Model -- Version 1 Specification", B. Moore, E. Ellesson, J. Strassner, A. Westerinen, February 2001

[3] GRES'01, "A "Policy-driven" approach of SLA Management", O. Poupel, A. Gonguet, December 2001

[4] IETF-RFC 2753, "A Framework for Policy-based Admission Control", R. Yavatkar, D. Pendarakis, R. Guerin, January 2000

[5] IETF-draft, "Policy Core Information Model Extensions", draft-ietf-policy-pcim-ext-07.txt, B. Moore, L. Rafalow, Y. Ramberg, Y. Snir, A. Westerinen, R. Chadha, M. Brunner, R. Cohen, J. Strassner, February 2002, work in progress, expire in August 2002

[6] DMTF, "Common Information Model (CIM) Specification", version 2.2, June 1999, http://www.dmtf.org/spec/cims.html

[7] IETF-draft, "Policy QoS Information Model", draft-ietf-policy-qos-info-model-04.txt, Y. Snir, Y. Ramberg, J. Strassner, R. Cohen, B. Moore, November 2001, work in progress, expire in May 2002

[8] NET-CON'2002, "Implementing a VPN service with policy rules", H. Abdelkrim, N. Verhoeven, October 2002

[9] IETF-RFC 2401, "Security Architecture for the Internet Protocol", S. Kent, R. Atkinson, November 1998

[10] IETF-draft, "IPVPN Policy Information Model", M. Iyer, A. Gonguet, C. Jacquenet, P. Lago, R. Scandarioto, February 2002, work in progress, expire in August 2002

SECURITY