Policy-Based Network Architecture

White Paper

Contents

1 INTRODUCTION TO POLICY-BASED NETWORKING 3

1.1 Goals of the Policy-based Network Architecture 3

2 BASIC MODEL FOR POLICIES 4

3 POLICY ENFORCER 4

4 POLICY MANAGEMENT 5

4.1 Policy Editor 6

4.2 Interface to a Directory Database 6

4.3 Policy Decision Administrator 7

5 QOS GATEWAY FUNCTIONALITY 10

6 BANDWIDTH BROKER FUNCTIONALITY 10

7 SUMMARY 11

1 Introduction to Policy-based Networking

Each day, companies strive to correlate business decisions to things that actually happen on their network.

- Selecting which users have access to which network resources
- Prioritizing which applications are critical to company operations
- Delivering tiered bandwidth and differentiated services to each customer according to their needs
- Managing the voice, video and data demands on corporate LAN and WAN links.
- Managing the overall flow of traffic through internal and external networks

All of these actions share a common requirement by applying corporate business policies to specific network actions including bandwidth management, firewalling, caching, routing and VPN equipment. Today, the network manager or network service provider must manage policies for all of these devices by managing a wide array of users, applications and resources to determine policies and then configuring each individual piece of equipment.

What is needed is a comprehensive, policy-based system that will allow the network manager to define, in a succinct and organized fashion, corporate policies that automatically effect change on specific equipment in the network environment. The end result is that the end-to-end network performance will meet the general expectations of the corporate, commerce or service provider environment.

In summary, business decisions, more and more, effect the entire network infrastructure. To manage today's business, the network must be reliable. The network must be predictable. To accomplish this, an overall end-to-end strategy must be developed to correlate the business with the overall network actions. This policy-based network architecture document details some of the goals and processes involved in developing this system. Allot's policy-based network system delivers a comprehensive architecture that allows the merging of high-level user, application and resource policy information with network-wide policy actions.

1.1 Goals of the Policy-based Network Architecture

The goals of the policy-based network architecture, outlined in this document, include the creation of a standards-based system that addresses both the enforcement and the administration of policies. Specifically, the system will perform various functions including:

- **Policy Administrator.** Creating a distributed, hierarchical system to coordinate and manage policies between policy management devices, directories and various policy enforcement devices using a standards-based architecture approach.
- **Interface to Directory Database.** Provides access to higher level, user and application-level policy information via data stored in common directory repositories. This high-level database information can then be translated into actual policy enforcement actions.
- **QoS Gateway.** Providing end-to-end policy enforcement and management via standards-based signal provisioning protocols including Differentiated Services, ToS, RSVP, MPLS and 802.1P
- **Bandwidth Broker.** Providing bandwidth brokerage services allowing an automatic system for multiple domains to negotiate service level guarantees.
- **Centralized Monitoring and Accounting.** Provides centralized policy-based accounting and remote monitoring services.

2 Basic Model for Policies

In a standard policy-based network, policies consist of two components.

- A set of ***conditions*** under which the policy applies. This might include parameters such as user name, addresses, protocols and applications types.
- A set of ***actions*** that apply as a consequence of satisfying (or not satisfying) the conditions including bandwidth guarantees, access control, service load-balancing, cache redirection and intelligent routing.

These conditions and actions consist of a series of passive and active components on the network. As a simple model, this would include a **policy manager** which is the central policy administration and directory repository point and a **policy enforcer** which consists of remote active management components that make up the local policy decision and enforcement points throughout the local wide-area networks.

3 Policy Enforcer

The Policy Enforcer can be a simple router that makes policy decisions based on a field in a particular "tagged" packet. Alternatively, the Policy Enforcer may be a piece of equipment that locally consolidates and analyzes traffic flows and network conditions in order to perform complex network actions such as:

- **Traffic Conditioning and Shaping.** This includes things such as traffic prioritization, traffic guarantees and bandwidth management
- **Policing.** This includes access control, user authentication and remote login
- **Tagging/Signal Provisioning.** This includes translating and relaying signal-provisioning information (RSVP, Differentiated Services, 802.1P, MPLS) through the network.
- **Server Resource Control.** This includes advanced enforcement capabilities such as server load-balancing and cache redirection.

Typically, this more complex piece of equipment will sit at the edge or border of a network domain and relay, via signaling protocols, overall bandwidth requirements to the internal network equipment. When referring to Policy Enforcement, this document refers primarily to these edge devices and, specifically, to the Allot AC Policy Enforcer System itself.

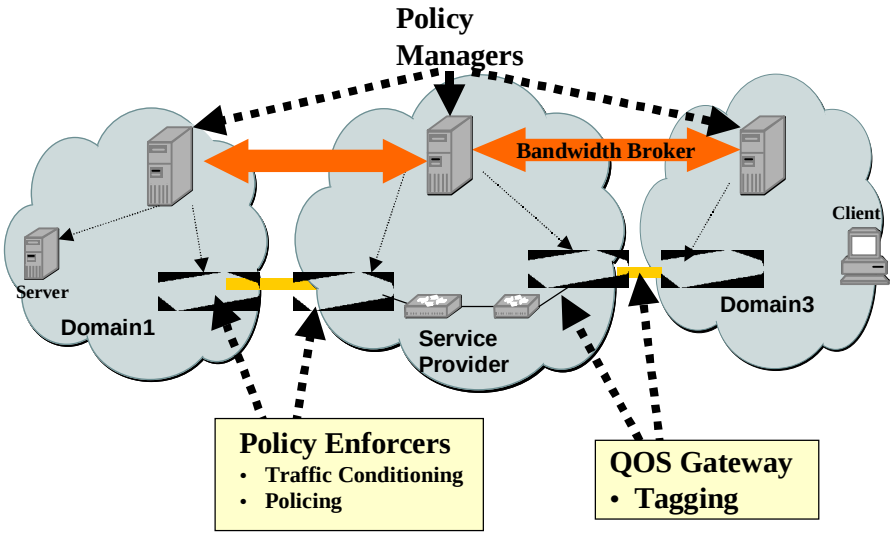

Figure 1. *The Policy Enforcer is placed at the edge of specific domains. It communicates with the Policy Manager to understand overall network policies and then performs various enforcement functions including traffic shaping/conditioning, policing and signal provisioning. The Policy Managers will communicate with each other for purposes of coordinating service level agreements and brokering bandwidth between the different domains.*

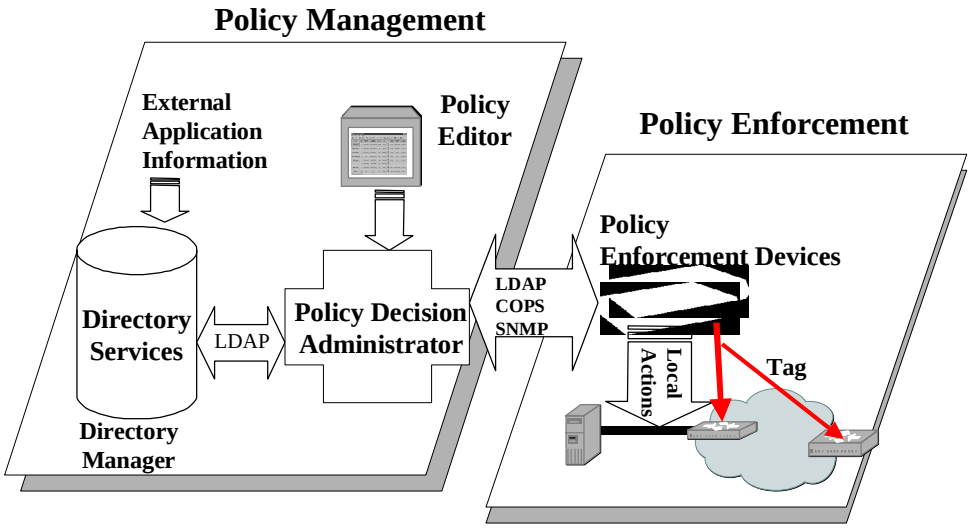

Figure 2. *The **Policy Management** functions are responsible for coordinating user input with other external and internal policy information into concise network terminology. This information is then relayed to the **Policy Enforcement** equipment for possible network actions.*

4 Policy Management

The **Policy Management** functions are responsible for coordinating administrator input with other external and internal policy information and translating this information into concise network terminology. The Policy Management service is responsible for coordinating the flow of bandwidth between various devices that make up the input and output to specific domains. By managing the critical border locations in a specific domain and then having the enforcement devices communicate, via standard signaling protocols to the internal devices, this system creates a complete end-to-end policy-based network solution.

Policy Manager functionality can be distributed and hierarchical in structure representing various physical and logical domains for management of specific Policy Enforcement devices. As an example, an enterprise domain can be defined for the whole corporation that includes general policies and management structure that effect every user, application or resource. Individual departments "inherit" the higher level corporate policies but can then define their own enforcement policies for the clients and servers that it controls. The corporate network administrator can delegate administration rights to the local department's administrator.

The Policy Manager consists of various logical pieces that can each run on separate servers or combine into a single system including the ***Policy Editor,*** the ***Interface to the Directory Database*** and the ***Policy Decision Administrator***. Each of these components is described in more detail in the following sections.

4.1 Policy Editor

The Policy Editor provides the network manager with capabilities to centrally configure rule-based policies that take high-level concepts and translate them to control of services within the network infrastructure. The policy-editor can be accessed directly by network managers for input via a Java/web interface or can be part of a centralized management structure provided by systems management products such as HP OpenView or Tivoli.

The editor will, in general, store information an LDAP-based database directory. Communication with the directory can be through the Policy Administrator or through third party directory applications. The Policy Editor will have added capabilities for translating generic policy information stored in the directory to actual policy rules.

4.2 Interface to a Directory Database Server

The Directory Database Server provides the central repository for policy information. In general, the Directory Database resides on a Directory Server as a third-party LDAP-based application provided via companies delivering directory-related products such as Microsoft, Netscape, IBM, and Novell. The Directory Server is responsible for the storage of a wide range of information including e-commerce, user login, and network yellow pages as well as network specific policy information. The directory can be grouped in a distributed and hierarchical fashion for sharing data.

The key to the directory is the wealth of applications that allow users to organize and correlate the wealth of information that subsequently gets stored into the database. A user can, for example, enter their entire customer list into the directory and then assign specific administrative and policy information on each customer including network specific bandwidth policies.

The directory will interface to the Policy Decision Administrator in order to create higher level, dynamic policies. An administrator will be able to define a customer as “gold level” and then setup a specific policy that says that all gold level customers will receive a specific priority throughout the network. Advanced features will allow the defining of dynamic policies that will allow network managers to script specific application conditions in order for a network action to take place. A network administrator, for example, would be allowed to assign a given priority to a customer who spent a minimum amount of money in the last year.

4.3 Policy Decision Administrator

The Policy Decision Administrator acts as a central command center for policies in the network:

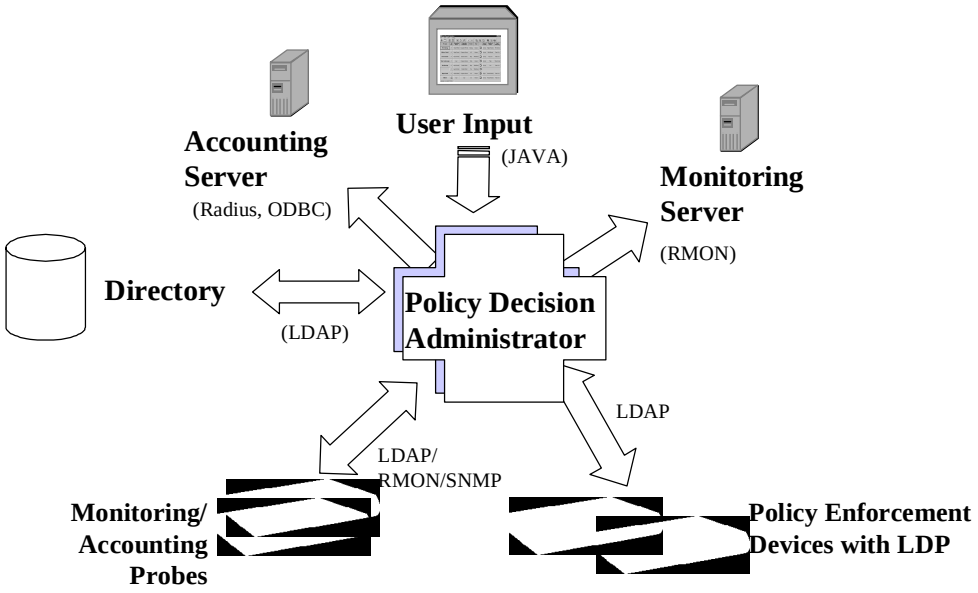

Figure 3. *The Policy Decision Administrator performs many functions including creating policies based on static information in the directory and other databases as well as transient information based on the status of the network. This information is then relayed to various policy enforcement devices for specific network actions.*

- The Policy Administrator translates policies stored in the directory service to network actions and policies.
- It discovers and identifies all policy manageable enforcement devices in its domain.
- It responds to requests from policy enforcement devices for specific policy information. In the case of nodes that have local decision capabilities, it will act as a higher level administrator of policies.
- It relays information to policy enabled network devices using standards-based protocols such as LDAP and COPS. This information, in general, is derived from information stored in the directory server
- It interfaces to Policy Editors allowing network managers to define specific network-wide policies and actions.
- It acts as a distributed collector of monitoring and accounting information.
- It provides added capabilities for coordinating discovery and management of specific policy enforcement devices. It tracks changes to the directory server and relays the information to the policy enforcers in its domain.

The Policy Decision Administrator is software-based and can run simultaneously on the directory server or as separate entities that communicate with the directory via LDAP. In some cases, parts of the administration functions may reside on one or more of the Policy Enforcers allowing the enforcer to run independent of external devices.

4.3.1 Decision Administrator Architecture

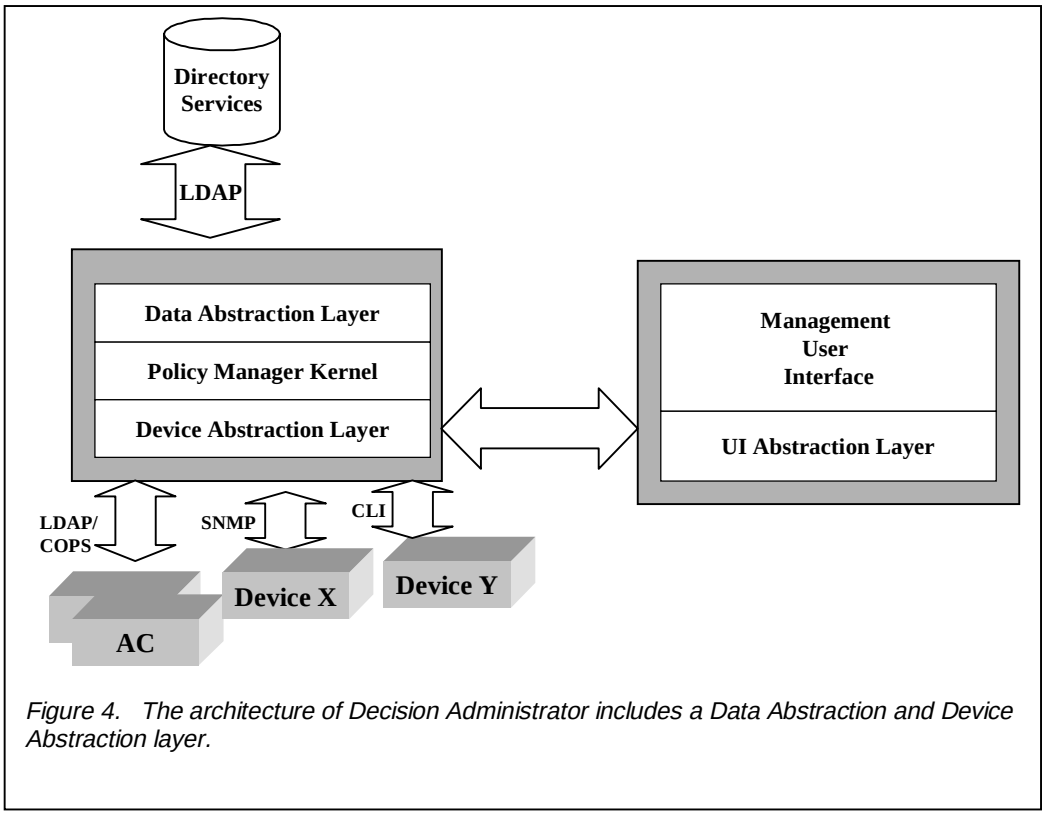

Figure 4. The architecture of Decision Administrator includes a Data Abstraction and Device Abstraction layer.

The Decision Administrator consists of various layers that provide policy management functions that interface to various components including the Directory, Enforcement Devices and the Management User Interface.

4.3.1.1 Data Abstraction Layer and Management Interface

The Data Abstraction Layer is the interface to the directory. It maintains and has knowledge of the policy structure and content. In its basic form, it allows abstract definition of policies defined in the directory to be translated to physical characteristics in the network.

A manager, for example, can define a concept of "Service Type" in the directory. He can then set a given **customer** in the directory to have a **Service Type** of, for example, ***Gold***. The Data Abstraction Layer then provides pre-defined and user-defined variables that define things such as:

- **Service Type** is an LDAP directory schema variable
- **Service Type** translates, in this case, **customers** into a concept an enforcement device can understand – namely a group of IP addresses
- A new entry called **Service Type** will now be accessible through the Policy Manager User Interface. It will serve as a new **Rule Condition** (along with things such as IP addresses, protocol types and time-of-day).
- The manager can now declare, using the Policy Manager User Interface that, as a condition, a **Service Type** equal to ***Gold*** will translate to a specific class-of-service. Perhaps, in this case, ***Gold*** would specify a minimum bandwidth of 128Kbytes/sec and a maximum burstable bandwidth of 256Kbytes/sec.

In this fashion, any variable found in the directory can be translated into a physical packet classification and result into actual network-wide actions.

4.3.1.2 Device Abstraction Layer

The device abstraction layer translates policies to specific device schemas and then relay this information to specific policy enforcement devices. For the near-term, there will be different types of enforcement products that will communicate with the Device Abstraction Layer in different formats and protocols. This may include protocols and architectures such as COPS, LDAP, SNMP or, for some legacy products, a command-line interface.

5 QoS Gateway Functionality

Policy Enforcement can come about by performing a specific service at the Policy Enforcer. Alternatively, simple policy devices, such as core routers, can make policy enforcement decisions based on information that is "relayed" through the network by various standards-based "tagging" or signaling protocols.

- **End-to-End signaling mechanisms**
  - RSVP.
  - Differentiated Services
- **LAN-based signaling mechanisms**
  - 802.1P/Q
  - MPLS

A Policy Enforcer can work as a QoS-gateway whereby it will translate and enforce end-to-end policies to each specific domain.

An NSP, for example, may want to have its own enforcement policies that say, "Premium Customers can use our high speed network link".

Specifically, the Policy Enforcer will perform these tagging/translation functions by:

- Identifying incoming packets that match user-defined policies and adding the appropriate signaling protocol to the local LAN.
- Identifying incoming packets that have a given QoS tag and, based on existing policies, perform local bandwidth management functions on the connection. The policy may say that "anything coming in from a specific customer with priority 3 will be guaranteed a minimum of 100K of bandwidth"

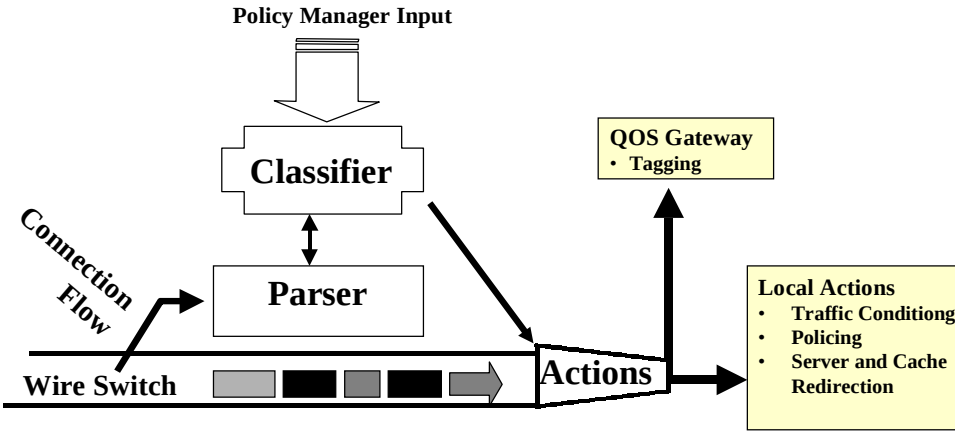

Figure 5. *The Allot AC System is an example of a Policy Enforcer. It contains special software for high-speed parsing, analyzing and classifying incoming traffic and then performing actions such as traffic shaping, server and cache redirection, monitoring and accounting. In addition, the AC system has the ability to perform QoS gateway functionality whereby it can translate and tag traffic according to standards-based signaling protocols such as Differentiated Services, RSVP and MPLS.*

6 Bandwidth Broker Functionality

The bandwidth broker allows various domains to automatically negotiate policies. An ISP, for example, can dynamically negotiate different service level agreements and committed bandwidth with a given customer. Alternatively, a server provider could charge different rates for bandwidth depending on the demand. To do this, the policy manager will contain the ability, using standards based protocols, to communicate with remote policy servers in order to negotiate the policy and with local enforcers to determine the state of the network.

The bandwidth broker will take into consideration the ability of the entire network to deliver the policy request. If a customer requests that its minimum bandwidth guarantees be raised from 128K to 384K, the bandwidth broker will check the state of the network over a long period, the maximum performance of the domain and the number of other guarantees that have been granted.

7 Summary

The key to aligning business goals with network resources is to define and implement a set of policies that map organizational and user goals and expectations with specific network actions. To simplify this process, Allot Communications has designed the Policy-Based Networking architecture that outlines a complete system for policy management. The Policy-based Network System includes an intelligent approach that combines:

- A centralized, distributed and hierarchical approach to network policy management using a directory database to organize the user, resource and general policy data
- A standard approach to network policy enforcement that performs both localized and end-to-end policy enforcement approaches. Functionality such as bandwidth management, server load-balancing, cache enforcement, VPN, firewall, monitoring and accounting can all be controlled using a single policy derived from the central policy manager.
- A complete system for defining high-level user and application concepts that can easily be translated to specific enforcement policies.
- QoS gateway and bandwidth management functionality to create a complete end-to-end system.

This system presents an overall business tool that allows corporations to organize business concepts with specific network policy actions.

United States:
292 E. Main Street
Los Gatos, CA 95030
Phone: (408) 399-3154
Fax: (408) 399-3164

Email: info@allot.com
WEB site: www.allot.com

Israel:
5 Hanagar Street
Industrial Zone
Hod-Hasharon
45800 Israel
Phone: (972) 9-744-3676
Fax: (972) 9-744-3626

Europe:
World Trade Center
1300, Route Des Cretes
BP 255
06905 Sophia Antipolis
France
Phone: 33 (0) 4 92 38 80 27
Fax: 33 (0) 4 92 38 80 80