



Policy.Net: Policy Based Network Traffic Management

OVERVIEW

Network access is an integral and often critical part of day-to-day business for most computer users. Response time, latencies, throughput, reliability and quality-of-service metrics gauge

Managing the network efficiently often defers the need to upgrade the network and reduces costs

a network's performance. Network architects and planners focus on operational cost, security, efficiency and manageability of the network.

Every user perceives the network differently and has a different set of expectations from the network. The network is not simply a physical media for information transfer. In a larger sense, the network is primarily a shared resource. When a resource such as a folder or printer is shared, access privileges and permissions are assigned to establish a policy for sharing. The policy based network access paradigm derives from the same principle. Traffic management transforms the network into a managed resource. Centralized policy management and stateful network interface provisioning are powerful strategies to regulate networks and control traffic load for performance, efficiency and security.

The rapidly emerging multimedia applications market in today's dynamic workplace has introduced serious challenges to network bandwidth on local area networks. A strategy to regulate and control the network resource efficiently is mission-critical for enterprise networks. Network bandwidth is a vital resource worthy of conservation. Managing the network efficiently often defers the need to upgrade the network and reduces costs. The 90's were a decade of abundance, as low-cost memory and faster processors promoted rapid sales of PCs to businesses and homes. As that trend curve flattens and budgets tighten, value-added services, performance enhancements and system optimizations become dominant factors with consumers. Judicious use of existing capacity and infrastructure provides better return on investment.

POLICY BASED NETWORK MANAGEMENT

The distinct characteristics of effective policy based traffic and network management are:

- Classification of network traffic (voice, data, audio, video, image, web, protocol etc.)
- Degrees of control (rate, time of day, congestion level, bandwidth etc.)
- Stateful traffic inspection
- User identification (IP address, hostname, login account)
- Application identification (well-known service, application type)
- Policy enforcement

The growing demands of today's diverse traffic spectrum on limited and expensive bandwidth require strategic controls to build a manageable network.

The most pragmatic and viable controls are those that are easy to understand and administer in a business environment and offer customizable and

The most pragmatic and viable controls are those that are easy to understand and administer in a business environment and offer customizable and flexible quality of network service to end-users based on legitimate requirements of the user

flexible quality of network service to end-users based on legitimate requirements of the user. The motive of an access control policy is to optimize use of shared resources amicably between users rather than impose restrictions.

The deployment of a wide variety of services and controls are possible through policy based network management:

- Centralized policy management (rules and directives that establish a network access policy)
- Distributed policy controls (local processor and memory resources)
- Scalability (number of end-users, end-nodes)
- Scope of control (user, node groups)
- User specific network privileges (roaming profile)
- Application specific network privileges (admission control, bandwidth)

- Traffic class restrictions (file transfer, email, web pages, chat etc.)
- Time and day restrictions
- Domain restrictions (network address and subnet mask)
- Site restrictions (allow, deny lists of URLs, IP addresses)
- Content restrictions (keywords, phrases with AND/OR operators, PICS ratings in web documents, email, etc.)
- Search restrictions (keywords patterns or sequences)
- Dynamic bandwidth management (bandwidth reservation, bandwidth on demand)
- Traffic priority (voice acceleration)
- Traffic recording based on triggers
- Network surveillance (status monitor)
- Violation reporting
- Alert notifications
- Traffic billing (budget allocation, accounting)
- Network congestion management

CLIENT BASED PARADIGM

Server based firewalls regulate network access without direct involvement of the end-nodes. This implies that the end node is essentially 'dumb'. While server based firewalls may be appropriate to

A comprehensive network policy must manage traffic not only at the backbone network and WAN access points, but also at the point of origin

restrict or deny external users access to the internal network at the edge-node, the strategy is inappropriate to restrict or deny internal users access to the external network. By contrast, a client-based policy shifts the onus of policy management to the 'smart' end-nodes. This approach supplements server-based firewall security (at gateways, proxy servers) and helps to alleviate poor response times, connection timeouts, traffic congestion and bottleneck delays at the server. The processor and memory resources are idle more often on end-nodes than at busy gateway servers. Conservation of intranet bandwidth and offloading of cumbersome user or application specific tasks from busy servers to client end-nodes significantly enhances network performance and throughput. There is a finite distinction between traffic management and network security considerations. The primary emphasis of Policy.Net is to regulate traffic flow as close as possible to the source. Server based corporate firewalls are designed specifically to deal with a network's security requirements. A comprehensive network policy must manage traffic not only at the backbone network and WAN access points, but also at the point of origin.

A proxy based firewall at a gateway acts on behalf of well-known applications for security and control. New services are denied until a proxy becomes available. A packet inspection based firewall requires application-sensitive modifications to the inspection code to provide maximum security and allow the new service to pass through the firewall. In a client centric approach, application specific inspection of content and access privileges for new services may be easily provisioned at the client without the need to modify client software.

NETWORK TRAFFIC MANAGEMENT

The nature of applications traffic may be characterized by constant or variable bit rate, continuous or bursty allocation of bandwidth, loose or continuous timing relationships between the endpoints

Bandwidth subscription coupled with traffic priority offers a dynamic and adaptive mechanism to manage the wide spectrum of traffic typical of network environments

and delay sensitivity. Local area networks lag behind modern broadband networks in quality-of-service and class-of-service technologies. The network policy must provision appropriate network access privileges and resources to service the differentiated types of traffic. Application-specific classification is important for sensible traffic load and bandwidth management. User-specific classification is pragmatic for authentication, security and assignment of preferential treatment to specific users.

Bandwidth reservation is a static control and does not address temporal traffic variations. Bandwidth subscription coupled with traffic priority offers a dynamic and adaptive mechanism to manage the wide spectrum of traffic typical of network environments. Relative priorities also alleviate the potential starvation of low priority traffic. The combination of priority and application based bandwidth allocation offers a flexible and intuitive method of resource management.

MANAGED NETWORK ARCHITECTURE

Policy.Net is a comprehensive policy based Internet access and network traffic management solution, available for deployment in businesses, schools, libraries, cyber cafes and homes as a SOHO or enterprise solution on all Microsoft Windows platforms (95/98/ME/NT/2000/XP). The system configuration is scalable and comprises of multiple policy execution points (or policy agents) and policy management points (or policy servers).

The Policy.Net agent/server model is analogous to the Common Open Policy Service (COPS, RFC-2748) client/server model. The policy control protocol is simple and extensible to

The policy control protocol is simple and extensible to support diverse client specific information and policy directives without requiring modifications to the protocol itself

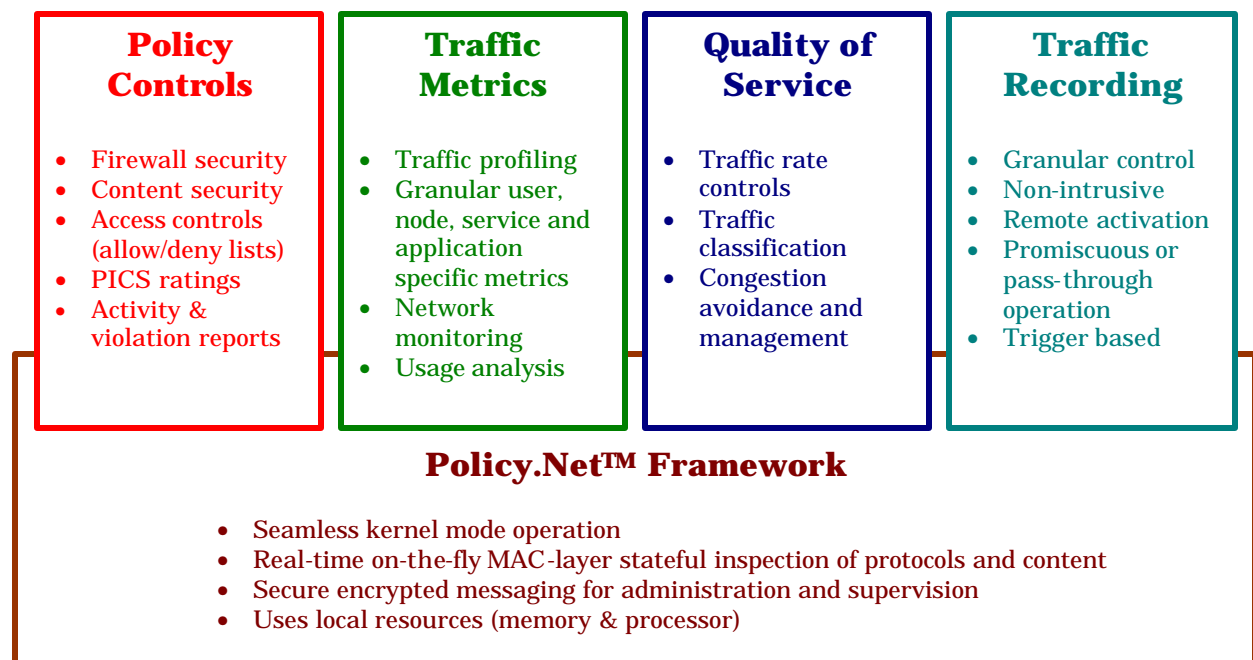
support diverse client specific information and policy directives without requiring modifications to the protocol itself. The protocol uses TCP as the underlying transport for reliable and secure exchange of messages between the policy server and the agent. The protocol provides message level security for authentication, replay protection, and message integrity. Secure ICMP messages are used for periodic lightweight supervision of agents.

DISTRIBUTED ARCHITECTURE

There are many disparate products in the market today, each designed to serve one specific purpose. No single solution exists to address a collective set of traffic engineering goals. Administration has

become cumbersome, complicated and highly technical. Training the staff to understand, correlate and maintain multiple solutions is expensive. The distributed Policy.Net architecture provides a single framework and modular services to simplify traffic engineering.

The distributed Policy.Net architecture provides a single framework and modular services to simplify traffic engineering



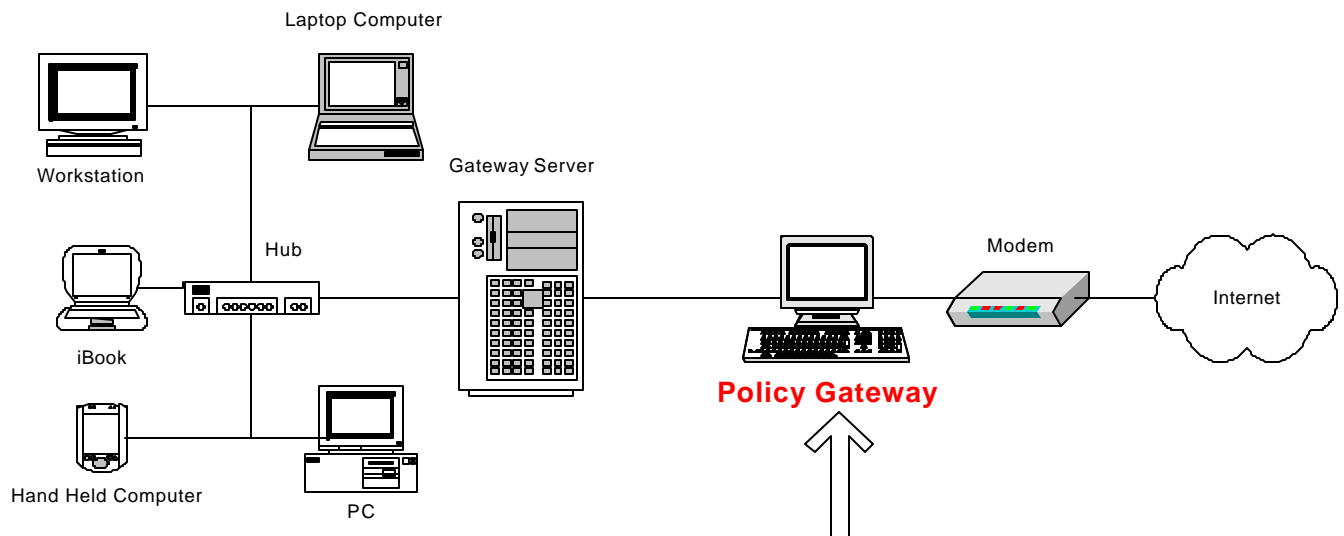
DEPLOYMENT CONFIGURATIONS

a) Policy Gateway

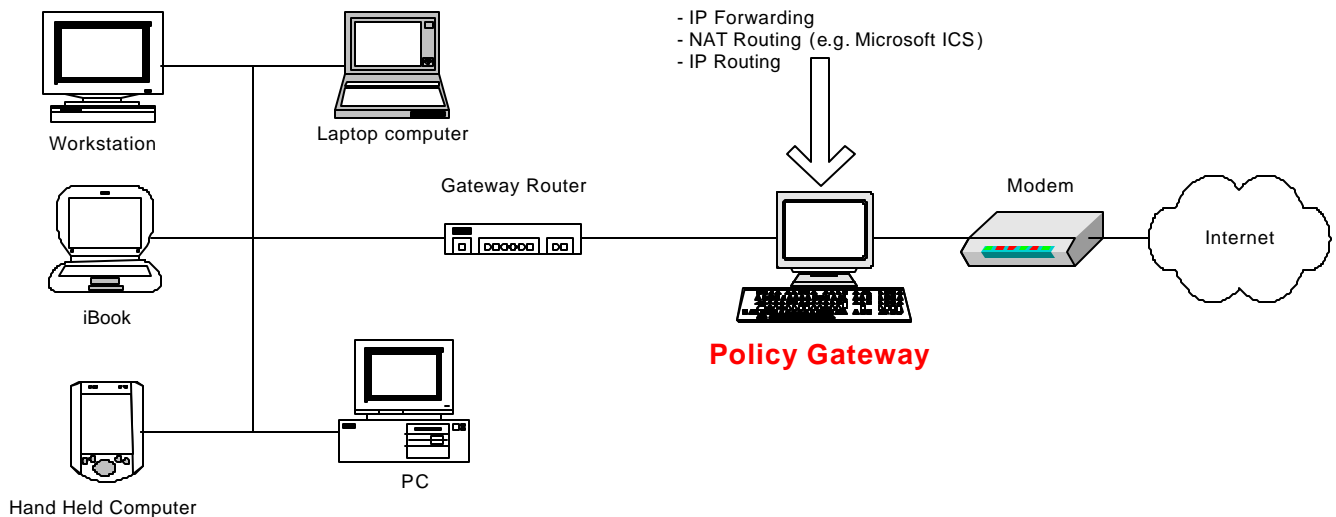
The Policy Gateway model is available as a per-server license and is intended for deployment in small office/home office environments, schools, libraries and home networks. This configuration supports all types of host end-nodes on the network (Microsoft Windows, Macintosh, Unix, Linux etc.).

Policy Gateway Configuration

This configuration comprises of a single multi-homed gateway node and multiple client end-nodes distributed on the local area network. Policy controls may be applied either by user logged on at the gateway node, or by host machine on the LAN.



If your existing network is configured for Internet access through a gateway server or router, you may deploy Safety.Net in any one of the following configurations:



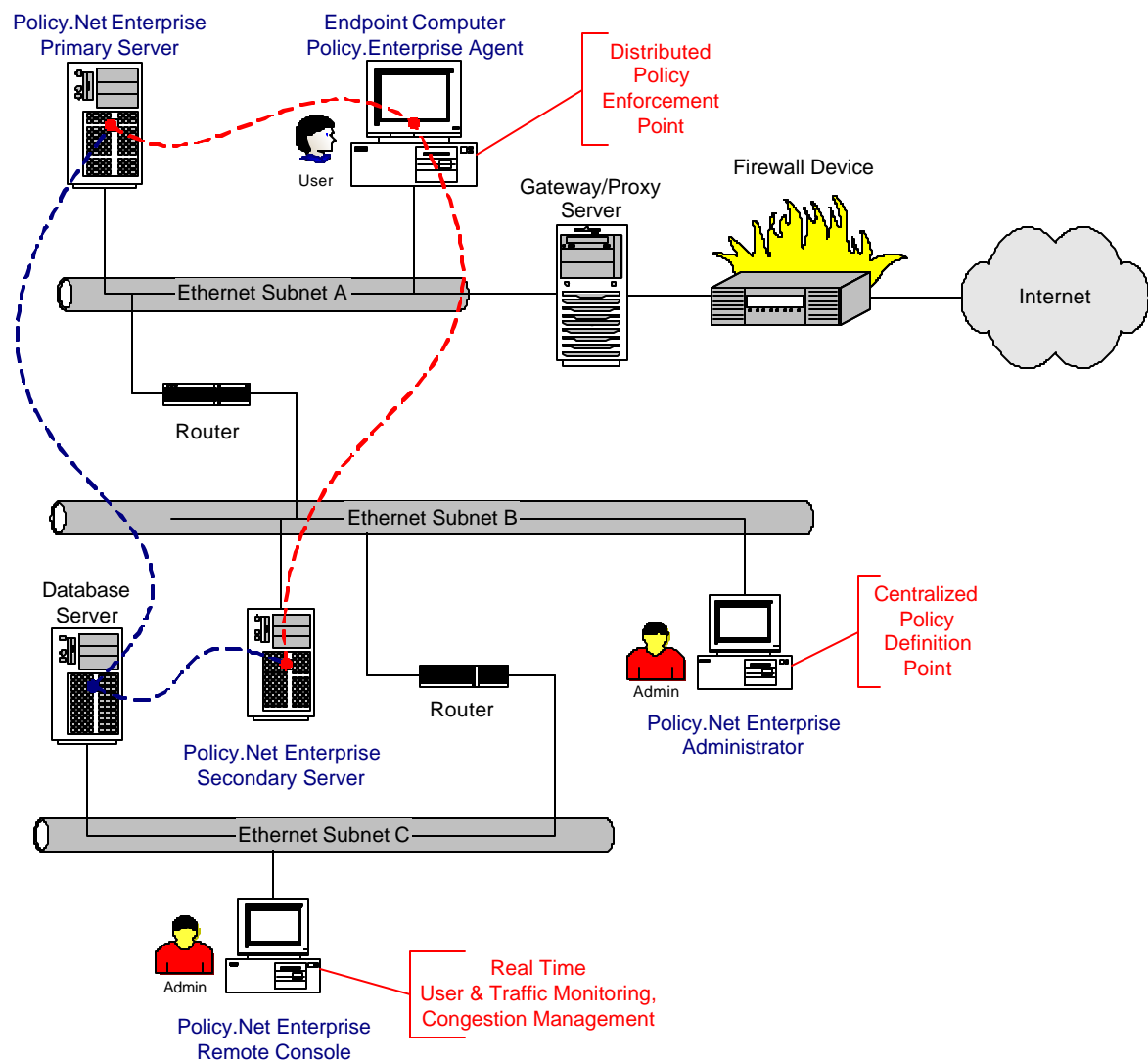
b) Policy.Net Enterprise

The Policy.Net Enterprise model is available as a per-seat license and is intended for deployment in business environments that require granular control of end-nodes and end-users. This configuration provides comprehensive traffic engineering controls.

Both configurations operate with any Proxy Server, Network Address Translation (NAT) Router, IP Router or Virtual Private Network (VPN) gateway from any provider.

Policy.Net Enterprise Configuration

This configuration comprises of multiple agents, policy servers, database servers and remote consoles distributed on the routed network.



POLICY AGENT

The policy agent is loaded at all endpoints or at a gateway. The agent is the regent for policy enforcement at the end-node. Policies defined for inbound and

The real-time engine at the agent enforces the policy through packet, application and session level filters

outbound traffic translate to a set of downloaded filters and feature activation controls for the local end-node or gateway agent. The real-time engine at the agent enforces the policy through packet, application and session level filters. Logging and live reports of alerts, violations and traffic records also occurs at the local endpoint.

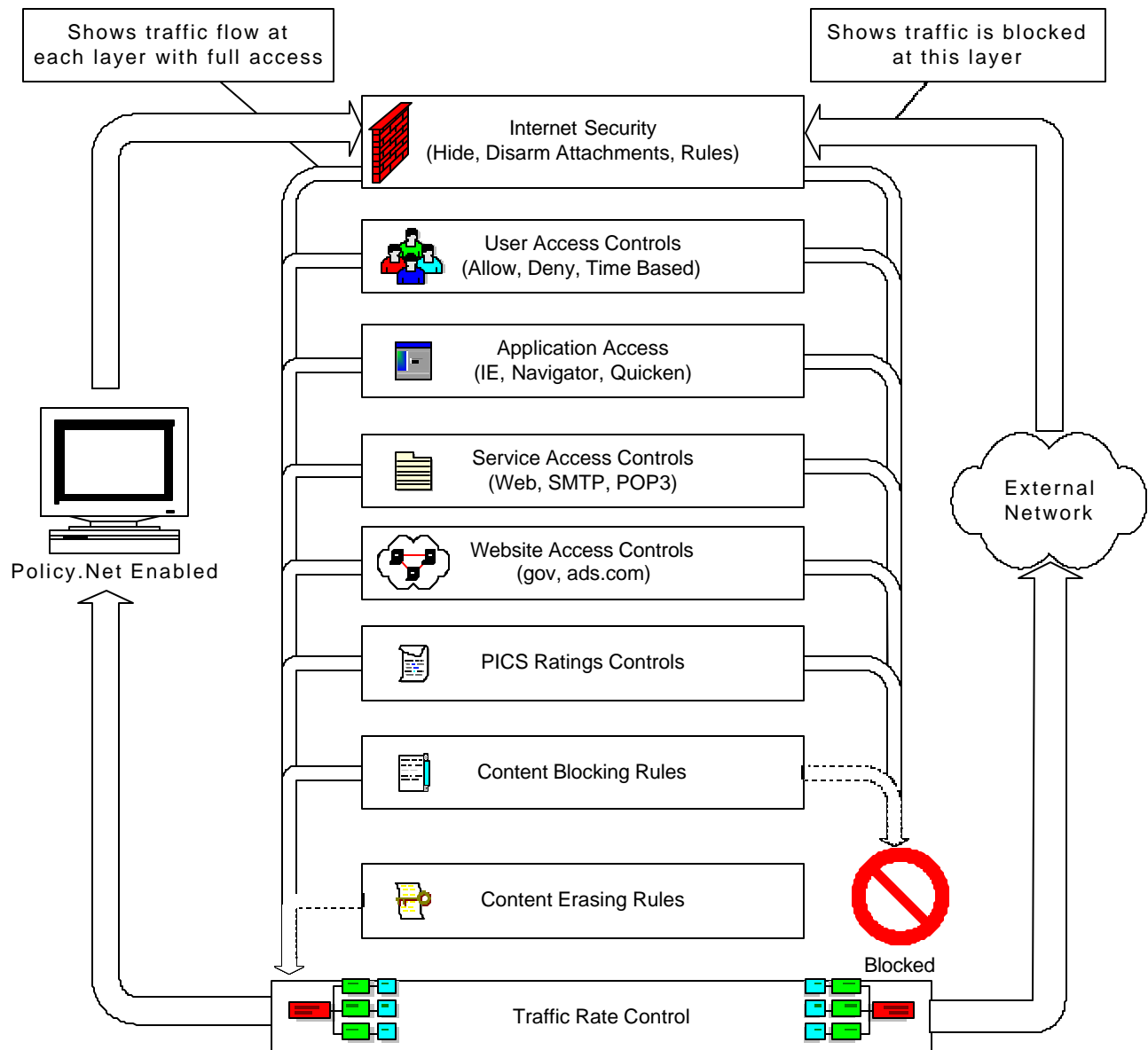
The clients in the Safety.Net configuration are distinguished by network address. The policy agents in the Policy.Net Enterprise configuration are uniquely distinguished by either a:

- a) User (logon name and domain),
- b) DNS Name,
- c) Network Address, or
- d) NetBIOS Name
- e) MAC Address
- f) Invariant ID
- g) Custom ID

The policy dilemmas that arise in situations where users must share machines and yet preserve individual access privileges are alleviated through user identification and roaming profiles.

As a performance optimization, a secure copy of the agent policy is cached at the local end-point. A digest of the cached policy is calculated and dispatched to the policy server for authentication, prior to enforcement of the cached policy. This mechanism serves to significantly reduce supervision traffic on the network and latency in policy execution.

ENDPOINT POLICY ENFORCEMENT



At each layer, Policy.Net enforces rules to determine whether to allow full access, deny or pass-through traffic to the next layer for further evaluation.

After all the rules are applied, the traffic flows through the rate control engine which enforces bandwidth privileges specified for the application or service.

POLICY SERVER

The policy server is a distributed set of services and database servers to manage agents at end-nodes on the network. Each of the policy server services may execute at a single server or on multiple servers (for load balancing) on the network, as a primary or backup service provider.

The policy server is a distributed set of managers and database servers to manage policy agents at endpoints on the network

The operations, administration and maintenance services provided are:

- a) Configuration Manager – Enumeration of remote agents and automatic distribution of end-user policies to the remote enforcement agents.
- b) Alert Manager – Logs alerts and violation reports dispatched by remote agents.
- c) Status Manager – Queries remote agents for verification of configuration and status at programmed intervals.
- d) Activity Manager – Records activity information associated with network transactions inspected at remote agents.
- e) Congestion Manager – Sends flow control directives to remote agents based on network congestion levels differentiated by traffic class (i.e. email, ftp, http, etc.). Queries and records traffic metrics from remote agents at programmed intervals.

The policy server uses a relational database to manage data sources for agent configuration and data.

REMOTE ADMINISTRATION

Management services are provided through a set of graphical user interfaces:

- a) Policy Administrator – Centralized definition point for users, computers, groups, policies and the assignment of policies to the endpoints.
- b) Remote Console – Management console for status monitoring, congestion control and remote traffic recording.
- c) Policy Monitor – Graphical 16-window customizable split screen charts for real-time activity tracking and network management.

CONTENT RESTRICTION

The pessimism and distrust associated with content blocking filters in cyberspace stems from fallible technology of the solution. The commonly cited weaknesses are:

Policy.Net addresses contentious issues associated with content blocking filters in cyberspace

- a) Covert enforcement of coded rules
- b) Inaccurate filters (excessively liberal or conservative)
- c) Silent denial of access (no user notification of reason)
- d) Use of inapt string recognition word filters to block objectionable content
- e) Promotion of default filters generated by “artificial intelligence” web spiders (amongst home users, parents rarely customize filters)

Policy.Net addresses these contentious issues with:

- f) Precision filters and open evaluation of filter accuracy through activity and violations reports
- g) Visible explicit allow/deny lists and restricted keywords (no hidden rules)
- h) User notification of reason for denial of access
- i) Context sensitive evaluation of objectionable content through content description in HTML headers, PICS ratings and phrase operators (AND/OR).
- j) No installation of default filters. Promotes proactive administrator involvement in values-based filter development through a user-friendly non-technical graphical user interface and scheduled activity reports via email.
- k) Content obliteration filters as a form of “limited restriction” for email, chat sessions and web pages.

While Policy.Net provides for the import and export of site lists and content keywords from outside sources, PICS ratings based blocking filters and content filters based on administrator discretion are highly recommended.

ACTIVITY REPORTS

Policy.Net generates connection level activity reports that may be dispatched to an email account or printed to hardcopy in detailed or summary formats at daily, weekly or monthly

schedules. The report includes granular and accurate connection level information about sites accessed, start time, stop time, total number of bytes sent and received, transfer rates, application that initiated the network activity, logged on user, attempted violations and blocking reason. This level of in-depth information is essential for network forensics.

***The activity report includes
granular and accurate
connection level information***

STATEFUL TRAFFIC INSPECTION

Packet filters operate on individual packets as a partial entity. The inspection of traffic content requires establishment of the proper context. State information allows interpretation of content in relation to the whole entity. Use of protocol state machines and content-sensitive parsers enables management of the entire session as one logical entity.

The real-time engine provides stateful traffic inspection of protocols and content in compliance with established Internet standards

The Policy.Net real-time engine provides stateful traffic inspection of protocols and content in compliance with established Internet standards.

- Hyper Text Transfer Protocol (HTTP, RFC-2068)
- Post Office Protocol (POP3, RFC-1939)
- Internet Mail Access Protocol (IMAP4, RFC-2060)
- Simple Mail Transfer Protocol (SMTP, RFC-821)
- Standard for ARPA Internet Text Messages (RFC-822)
- Transport Control Protocol (TCP, RFC-793)
- File Transfer Protocol (FTP, RFC-959)
- Hyper Text Markup Language (HTML, RFC-1866)
- Multipurpose Internet Mail Extensions (MIME, RFC-2045/2046/2047)
- Platform for Internet Content Selection (PICS, W3C Consortium)
- Internet Control Message Protocol (ICMP, RFC-1885/1256)
- Domain Name System (DNS, RFC-1035)

NETWORK CONGESTION MANAGEMENT

Policy.Net provides a mechanism to throttle the flow of traffic at network nodes through policy based controls. During periods of heavy congestion, directives are dispatched to the remote agents to step-

down traffic load to the network. As network congestion subsides, directives are dispatched to step-up traffic load until the normal level of traffic is restored. Rate controls derived from traffic classification and prioritization facilitates meaningful congestion management.

Rate controls derived from traffic classification and prioritization facilitates meaningful congestion management

AGENT TRAFFIC RECORDER

The Policy.Net Agent Traffic Recorder provides network administrators, engineers and developers the ability to monitor and analyze traffic at remote end-nodes through services provided at the remote agent. The traffic recorder's non-promiscuous mode of

The traffic recorder's non-promiscuous mode of operation is non-intrusive on broadcast network traffic and provides better granularity and performance compared to traditional promiscuous mode network monitors

operation is non-intrusive on broadcast network traffic and provides better granularity and performance compared to traditional promiscuous mode network monitors. The standard PCAP/TCPDUMP format capture file may be imported in third party tools such as Ethereal for detailed traffic analysis. The top-end network analyzers are bulky, expensive and difficult to operate. The cheaper alternatives are generally not applicable to less common network media configurations. The Policy.Net traffic analyzer is a cost-effective, easy-to-operate, flexible alternative that works with a wide range of media types.

REMOTE ACCESS MANAGEMENT

Server-based firewalls may not regulate and control direct network access through dialup, DSL or cable modems at an end-node. This uncontrolled dial-in/dial-out capability

Policy.Net regulates and controls remote network access through dialup adapters and VPN connections over the Internet

opens an avenue for intruder access and creates vulnerabilities. Policy.Net regulates and controls point-to-point network traffic and helps to plug a security loophole. The network policy can prohibit use of unauthorized modems attached to client end-nodes at the site or record suspicious activity.

Virtual Private Networks (VPN) technology allows remote clients to connect to the corporate network through VPN gateways. Though VPN clients use a secure connection to access their corporate network, the public IP address space leaves remote users vulnerable to hackers and intrusion attempts on the Internet. Policy.Net enforces policies on remote clients to plug security holes associated with accessing a VPN through an Internet service provider (ISP).

SYSTEM SECURITY

Policy.Net uses state-of-the-art encryption and cryptographic technology to enforce security and ensure integrity of user administration, supervision and authentication. Periodic

State-of-the-art encryption and cryptographic technology enforces security and ensures integrity of user administration, supervision and authentication

challenge-response handshakes and heartbeats between the policy server and agents, and digital signatures of agent configuration offer protection from hacker attacks and computer savvy workarounds. Privacy is enhanced through filters that block the covert transfer of local machine and personal user information over the Internet that may be abused by hackers.

SYSTEM RESOURCE REQUIREMENTS

The Policy.Net design is conservative in the use of critical shared system resources. Policy enforcement is performed in the kernel mode at the network layer. The effective use of non-

The effective use of non-paged system memory and algorithms for incremental packet content analysis are key to real-time performance

paged system memory (eliminates latencies associated with virtual memory access) and algorithms for incremental packet content analysis are key to real-time performance (no noticeable delay to user).

A minimum 32MB of memory and a 486/Pentium processor is recommended. The system configuration must simply satisfy the minimum system requirements of the underlying Windows operating system. As the Policy.Net engine operates below layer 3 of the OSI protocol stack, automatic physical media detection has been provided for deployment of Policy.Net on 802.3 Ethernet, 802.2 LLC/SNAP, 802.5 token-ring, FDDI and 802.4 token-bus configurations.

Additional memory may be required for a gateway configuration based on the volume of server traffic and number of client machines on the network. A multiprocessor platform is highly recommended for performance enhancements in heavy traffic environments.

ABOUT NETVEDA

NetVeda is a privately owned New Jersey based networking company developing solutions that provide granular and accurate traffic control for effective network management, improve quality of service (QoS) and optimize bandwidth resource utilization for Internet Service Providers (ISP), Small Office/Home Office (SOHO) and Enterprise network environments. NetVeda has pioneered solutions with adaptive incremental technologies to provide cost-effective and reliable policy-based network access, QoS, content and transaction controls. Our unique multi-platform kernel mode solutions execute below the network layer to minimize operational overheads and render real time performance with minimal impact on system performance.

NetVeda

<http://www.netveda.com>
<mailto:info@netveda.com>