

Endpoint Based Policy Management: The Road Ahead

Introduction

In a rapidly growing and crowded security solutions market, organizations need to deploy the most effective technologies taking into consideration the legitimate needs of mission critical applications, cost effectiveness and effort to install and manage the solution with minimum in-house administrative overhead. This document assesses the effectiveness of endpoint based policy management as a means of achieving higher application performance, simplifying management and maximizing security on an enterprise-wide basis.

The Need For Endpoint Based Policy Enforcement

Security on the Internet has been increasingly tightened motivated largely by the alarming number of malicious hacker attacks and intrusions reported almost everyday. However, absolute security requires trustworthiness at all points of vulnerability. Evidence shows that hackers are getting bolder and smarter everyday. A hacker needs to penetrate the defenses just once, whereas the technology to block intruders and hackers has to work all the time. There is no such thing as “perfect security”. While the response time to deploy protective measures against newly emerged threats has come down significantly, to perhaps minutes from days, it is inevitable that a new threat is likely to surface any second.

The least protected entity in today’s networked world is the endpoint (hosts) from which all forms of electronic commerce, on-line transactions and business activities are initiated. Defending against cyber attacks requires proactive risk mitigation, multiple layers of defense, and dynamic rather than static policies to thwart the constantly improvising attacker. Once an attacker has infected one vulnerable endpoint, the threat can propagate rapidly to other vulnerable endpoints and eventually challenge mission critical networks and servers.

Today, risk management measures in the industry are instigated by legal mandates and not merely by common-sense best practices for better consumer information and network security. Needs based adaptation at the endpoint is required to achieve a delicate balance between security and performance considerations.

Application Firewalling Increases Security

The threat posed by an infected endpoint to the corporate network is as real as a direct incoming attack. Hackers are increasingly penetrating through the HTTP, SSL, IM and SMTP firewall “holes” to attack endpoints which then become the staging ground for subsequent coordinated attacks on hosts on the internal network. The increasingly common practice of plugging mobile and wireless laptops, which easily evade server-based firewalls and are vulnerable to Trojans and worms, into corporate networks demonstrates serious security loopholes in network admission policies.

While security is very critical, it is not the only important factor to be considered. CPU intensive calculations and complex policies required to detect and block malicious activities are better performed at the endpoint than at gateway servers, proxies or Internet routers. A distributed approach offers better risk mitigation and performance compared to centralized processing. Application firewalling and stateful connection level traffic inspection at the entrance to the network is more efficient and effective at detecting and blocking harmful network-aware applications and activities.

Network Optimization Improves Application Performance

A centralized solution increases the processing overhead on traffic monitoring and policing servers in the flow-path. This reduces traffic throughput and increases end-to-end queuing delays, especially at Fast/Gigabit Ethernet line speeds. Offloading CPU intensive operations to the endpoint eliminates performance bottlenecks at server-based choke points. As the nature and magnitude of emerging security risks increases, the performance factor becomes significant as tighter budgets make it harder to

upgrade computers and network equipment to defend adequately against rapidly evolving threats.

Multimedia services such as streaming audio and video are not resilient to variable transit delays and require end-to-end quality of service guarantees for optimal performance. With the advent of IP phones and multicast audio/video conferencing services at the desktop, optimization of network traffic is fast becoming a necessity “on the last mile”.

Endpoint-based distributed policy enforcement and centralized policy definition offers an effective, scalable and cost-effective solution for small, medium and enterprise office environments.

Detailed Activity Reports Aid Forensics

The most effective defense strategy is to monitor traffic, analyze activities, enforce policies and report violations to facilitate constant evaluation of the effectiveness of current policies. While many products claim to provide in-depth information, only detailed connection level information is valuable for network forensics to detect and correct the root cause of security lapses and vulnerabilities. While vast amounts of traffic data may be mined and archived, real-time analysis and reporting of the information is extremely vital to facilitate rapid administrative intervention to engage emerging threats and violations through policy evolution.

Endpoint Based Policies Simplify Network Administration

Over-restrictive policies at firewalls and proxy based servers block legitimate business activities. Tuning policies at a single point in the flow-path for endpoint-specific privileges is difficult to administer in any enterprise-wide network. Besides, server-based solutions cannot offer preferential treatment for specific trusted applications, as only service level identifiers (e.g. TCP/UDP port numbers) are available at transit points.

Application trustworthiness is the ultimate control for tighter network security. Damage control is an absolutely essential component of risk mitigation. Blocking malicious applications at the endpoint is the “first layer of defense” in multi-layered security.

Endpoint Based Policies Improve Quality of Service

Packet marking for differential services on the broadband is a critical aspect for quality of service. Multimedia services rely heavily on low transit delays and high throughput guarantees. IP packets travel through a maze of internetworking devices, and undergo service and protocol conversions, as they get routed over MPLS, ATM or Frame Relay based carrier networks. Enabling packet marking at the endpoint, based on the needs of a specific application and class of traffic, improves end-to-end performance. Server-based security solutions and content engines integrated with router devices are not capable of determining whether a packet that bears the signature of a specific protocol (e.g. HTTP, SSL, IM, SMTP, etc.) was sent by a legitimate network application or harmful application at the endpoint. Malicious applications can easily mimic trustworthy traffic patterns and be granted preferential treatment!

Endpoint Based Policies Foster Positive Policing

Security fears (risks) often over-shadow legitimate performance requirements of network-enabled applications. Only endpoint based policy enforcement offers both application performance enhancement and trust verification to meet security requirements. Security may be enhanced one notch higher with remote peer screening that blocks trusted applications from establishing connections with untrusted remote nodes (a far-fetched concept for server-based and mid-stream solutions!). The processing overhead and queuing delays at server-based centralized solutions degrade performance of legitimate network applications. Packet marking at downstream network elements in the flow-path (e.g. edge nodes) does not compensate for the lack of quality of service enforcement early in the flow-path. Besides, policies enforceable at edge nodes have no application level sensitivity and only offer class of service recognition based on well-known port numbers for class-based queuing and empirical packet-

discard algorithms. Internet routing devices cannot implement CPU intensive complex policies.

Endpoint Based Content Inspection Protects Intellectual Property

Content engines in integrated routing devices and embedded firewall devices only process packet headers and not the entire payload. CPU intensive “deep content inspection” is only feasible at the endpoints. Payload inspection requires stateful inspection of protocols and MIME content at the connection level. This is a CPU and memory intensive function too overwhelming for mid-stream multi-function and multi-protocol network elements. Protection of intellectual property requires context-sensitive content filtering to detect and block file transfers and restricted content in electronic conversations (e.g. chat, instant messaging, email).

Summary

The architecture of enterprise networks is evolving to strike a delicate balance between performance and security considerations. A software-only solution at the endpoint offers cost-effective, application aware, and needs based policy enforcement compared to server or hardware based mid-stream devices. Only distributed policy enforcement points (PEP) with a centralized policy decision point (PDP) offer closed loop dynamic controls, to throttle endpoint traffic at the source in real time, to effectively manage server and network congestion. Contrary to common misconceptions, distributed traffic management solutions reduce administrative overheads and are simple to deploy and manage in enterprise networks. Endpoint based policy management solutions may be deployed alongside any existing gateway firewall (DMZ device) to enhance network security and end-to-end performance for mission critical network activities.