Resolving the Security Threat

Deep Packet Inspection for Residential Gateways

Residential gateways (RGs) have evolved dramatically over the past decade into devices that support time-sensitive and higher-bandwidth applications. RGs are now capable of delivering a vast array of services – such as Voice over Internet protocol (VoIP), advanced IP Television (IPTV), and security services.

Web 2.0 is driving even more new applications – such as peer-to-peer content delivery – which introduce significant security threats. As a result, service providers need complex RGs that can deftly handle new applications while safeguarding users from potential security breaches.

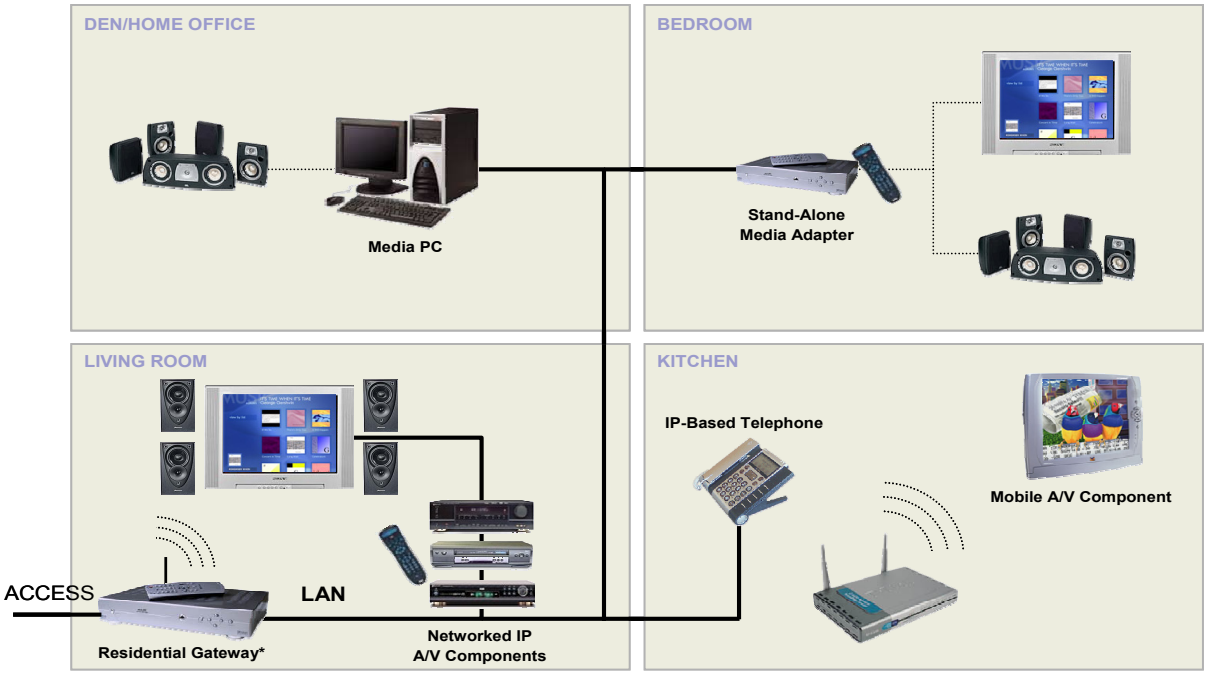
As a measure to counter the hacker-menace, this document dwells in depth on a key technology: Deep Packet Inspection (DPI). DPI uses packet payload inspection to prevent hackers from attacking end nodes and prevents hackers from manipulating service delivery parameters and impacting QoS requirements of sensitive traffic.

Table of Contents

The Pivotal Role of RGs

The capabilities of today's RGs have become pivotal to service providers' success. Service providers increasingly rely on the RGs to deliver the best Quality of Service (QoS) and highest level of security for delivering services to the networked digital home (**see** Figure 1). The gateways help service providers reduce churn, grow their subscriber base, and sell additional services, which in turn improves Average Revenue Per User (ARPU). Service providers are also expanding this vision to address the needs of the Small Office/Home Office (SOHO) and Small-to-Medium Enterprises (SMEs). Providing the expected Quality of Experience (QoE), while delivering advanced applications, is critical for ensuring a service provider's continued and successful growth.

Figure 1: A Networked Digital Home



Security: Beyond VPN, IPSec, and Encryption

A key element essential to ensuring QoE is the overall security framework of the service providers' network. Moving beyond the traditional Virtual Private Network (VPN) model, service providers must now address current and next-generation policy-driven content processing security framework. While the VPN model provides a certain degree of security using IPSec protocol and includes packet authentication and encryption mechanisms, it does not fully address security threats like denial of service attacks that exploit protocols and packet payload embedded signature-specific threats.

Need of the Hour: Comprehensive Security Framework

Hackers can impact QoS in several ways, from manipulating a given packet header to exploiting protocols. A comprehensive security framework must protect against IP header checksum anomalies, header options and spoofing, IP fragment attacks involving buffer-full conditions, over-run and over-write conditions, Internet Control Message Protocol (ICMP) anomaly protection involving large ICMP packets, and denial of service attacks that originate from Universal Datagram Protocol/Transmission Control Protocol (UDP/TCP) operations. In addition, the security framework must track URLs that are accessed to block unwanted access.

However, there is a key technology that supports a policy-driven content processing security framework: Deep Packet Inspection (DPI). DPI uses packet payload inspection to prevent hackers from attacking end-nodes, and prevents hackers from manipulating service delivery parameters and impacting QoS requirements of sensitive traffic.

DPI and Its Scope

DPI is a mechanism of examining the packet from Layer 3 to Application Layer 7. It involves not only Layer 3 to Layer 7 protocols, but also examines signatures in the content and behavior of the packet flow and protocols. DPI engines perform operations on the packet payload by applying a set of policies and comparing against a set of rules. DPI-based security frameworks maintain states across all packets in a flow and all flows in a given gateway system. DPI-enabled RGs make decisions, such as, packet drop or forward, based on the positive identification of any signature and rule or policy-match that takes place while examining the packet payload. These RGs also look for specific signatures in the content and generate events and alarms accordingly. The signatures often can be represented by an expression instead of just a simple character string.

DPI scans every packet in its entirety. Because services deployed to the digital home and SOHO/SMEs include time- and-latency-sensitive traffic, DPI requires minimal overhead and its implementation needs to be highly optimized.

DPI Operations

High-performance DPI is a challenging task because several factors can complicate its implementation. For example any IP packet can be exposed to numerous threats and the packet examination process gets complicated because of the multiple operations involved that includes:

- **Comparison against numerous signature-connected threats, which continue to grow over time as new threats arise**
- **Several rule checks, each with many signatures, since each packet can potentially create multiple attacks**
  A packet inspection mechanism must ensure not only a set of rules and signatures that are compared for attack identification, but also they must prevent multiple attack scenarios arising from an incoming IP packet.
- **Analysis of complex signature patterns**
  These patterns can be simple fixed strings or correlated patterns that require examination of certain group of patterns occurring in sequence. Another possibility is a pattern or group of patterns that can be expressed in a form of regular expression.
- **Byte-by-byte examination**
  As it is impossible to know the exact location of the pattern in the packet payload that could result in a security threat, every byte must be examined. These patterns can go beyond a single IP packet fragment or packet boundary.

DPI in RGs

As each byte is scanned for signature and rule check, DPI can result in higher CPU execution-time. However, DPI is extremely important for service providers who want to successfully deploy next-generation services. Since residential gateways are deployed and managed by emerging remote management frameworks like TR-69, it becomes a mandatory requirement to incorporate this comprehensive security framework in the RGs and extend the remote management framework to include a security-specific management information database.

Applications that Can Use DPI

A number of key applications – such as Intrusion Detection/Prevention Systems (IDS/IPS),

antispyware, spam detectors and antivirus – can leverage DPI. SNORT is one of the most popular IDS/IPS implementations providing a framework and an approach to detecting spurious actions that result from protocol anomalies and signature patterns embedded in an IP packet. IDS/IPS is one of several applications that leverage a payload inspection mechanism like DPI.

DPI plays an important role in "unified threat management". This term describes a solution that can provide comprehensive broad-based security applications from a single device. A unified threat management solution also may integrate network firewalls, advanced stateful firewalls, system logging, and packet traces.

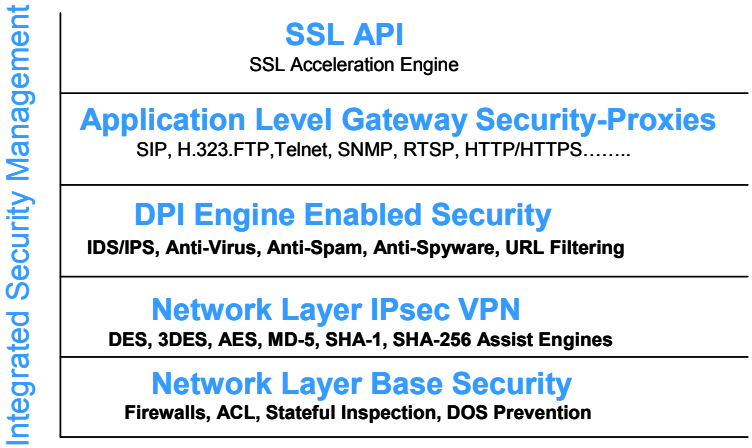
Next-Generation RGs for Guaranteed Delivery

As RGs continue to evolve, they will not only incorporate interfaces for high bandwidth access and home area network but also, from the service integration standpoint, will go beyond triple-play and include the system-level infrastructure needed for supporting unified threat management (**see** Figure 2). Such integration is essential for ensuring reliable and guaranteed service delivery.

Layer 3 to Layer 7 Security

While an overall security framework still requires the functionality of firewalls, advanced stateful firewalls, and a comprehensive set of policy-based access control lists, their effectiveness is limited because they are dependent mainly on packet header parameters. To be effective, service providers must ensure security from Layer 3 to Layer 7 by comprehensively examining the entire packet.

Figure 2: RG Integrated Multi-Level Security Framework



SoC RGs with Hardware Engines

The foundation for integrated RGs includes complex and highly efficient System on Chip (SoC) devices. Residential gateway SoCs are purpose-built network processors that, unlike current generation processors, integrate sophisticated engines to execute performance-intensive expression-processing algorithms inside the device. These devices are expected to scale in processor clock speed operating up to 1 GHz, which is equivalent to that in general purpose computing environments.

In order to tackle the issue of high performance, while carrying out deep packet inspections, gateway devices of the future are not expected to implement purely software-based DPI mechanisms. These next-generation gateway processors are expected to support DPI hardware-based-assist engines to help speed up the payload scanning process. All security applications will exploit a DPI-assist engine while carrying out payload inspection operations. This DPI engine

needs to be programmable in order to provide added flexibility to accommodate scanning algorithm requirements.

A Prospective Partnership Among Different Vendors

These advanced RGs are expected to provide a rich set of middleware, Application Programming Interfaces (APIs) and an effective toolkit infrastructure for DPI engines, so that third-party security application software can be integrated effectively and quickly. As a result, RG processor developers would ultimately support a partnership ecosystem focusing on software vendors who offer antivirus, spyware, spam filters, and IDS/IPS application packages. The partnership between security application developers and RG processor vendors enables fully integrated and well-tested security-application-support offerings to RG system vendors and service providers.

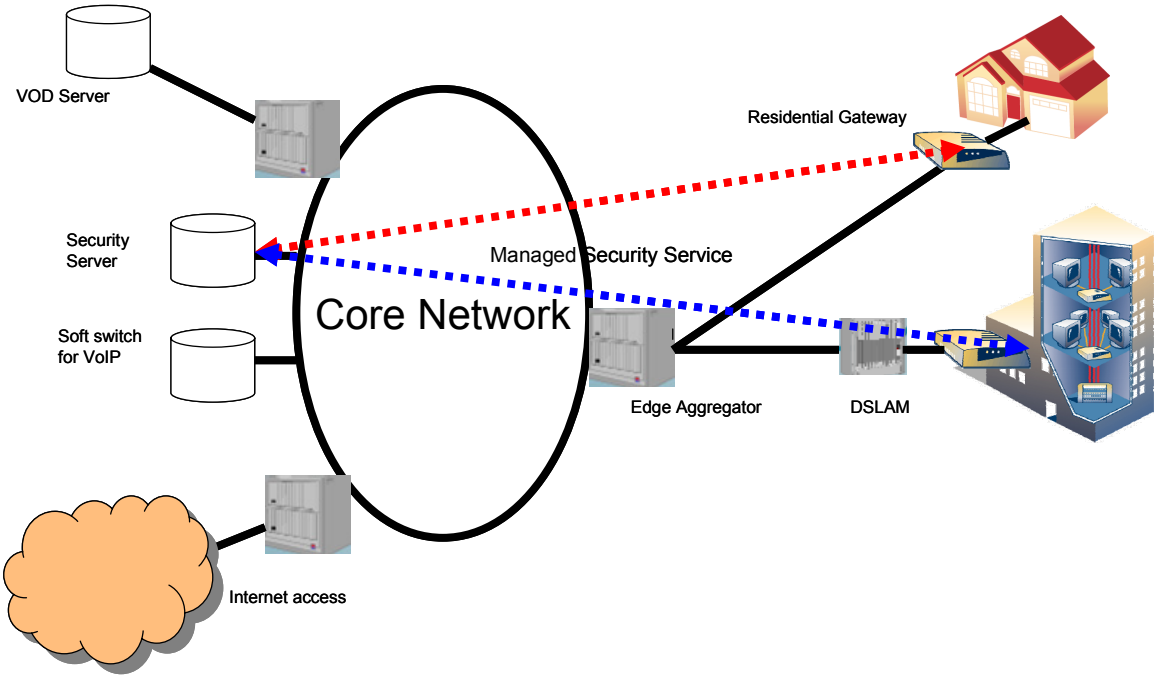
The Visage of Next-Gen RG

Next-generation RGs are also expected to offer native standard operating systems like Linux – integrated with publicly available open source SNORT-based IDS packages, including antivirus agents like ClamAV. These systems leverage next generation gateway silicon devices incorporating sophisticated DPI engines and support flexible policy languages that facilitate rule creation. The rules, in conjunction with software, help optimize DPI engines for effective content filtering, performance monitoring and attack reporting. However, RG architecture needs to scale to gigabit speeds to derive various policy decisions to ensure service level agreements are complied.

Secure Digital Home Network

Emergence of these advanced RGs provide an opportunity for service providers to deliver an integrated triple-play-service offering combined with a broad set of unified threat management services to secure the digital home and SOHO/SME. Figure 3 depicts such a network deployment.

Figure 3: Managed Security Service Model



The Agenda for Service Providers

Service providers must deploy systems that natively support architectures designed to incorporate engines, like DPI, to ensure their systems do not quickly become obsolete and require replacement. With the advent of standardized and centralized network management systems, service providers could ultimately deliver managed security services to compliment their current triple-play-service offerings. By doing so, service providers will be able to differentiate from their competition as well as minimize churn in the residential and enterprise subscriber bases and increase revenues with new and profitable offerings.

Vertically integrated service providers are also moving up in value-chain by deploying video servers and their associated ecosystem. With DPI and unified threat management, service providers can now integrate security servers in their core infrastructures that effectively interwork with their deployed RGs and SOHO/SME gateways. Such integrated security servers can track events/alarms generated by premises gateways upon positive identification of signatures embedded in the packet payload or upon abnormal traffic flow conditions. The core security server can initiate appropriate actions based on the configured policy devised during the SLA generation process with an end-user. In short, security service is no more a desirable feature for next-generation gateway systems, but it is an essential requirement to help sustain and manage QoE to an end-user

DPI Deployment Scenarios

Service providers can deploy DPI-based security network elements in two ways. In one scenario, the security framework is integrated into RGs and SOHO/SME gateways. Alternatively, it can be integrated in the last-mile edge network elements.

Advantages of RGs with Integrated Security Framework

There are advantages in integrating a security framework in RGs because these gateways have now become a nodal network element where both access network and home area networks terminate. Also the application environment is changing with the emergence of peer-to-peer applications, resulting in increasing traffic flow in both downstream and upstream directions. When there is an increased traffic in the upstream from the home, this traffic can potentially be the source of security threat. As security threats can emerge from systems inside home and enterprises, it is important for service providers to block spurious traffic flow at the RG, which is the aggregating point where subscriber traffic moves onto the service provider network. Putting the DPI-based security framework in an RG helps ensure that first-mile network elements, like DSLAMS, multiple dwelling unit (MDU) equipment, and second-mile metro edge aggregators focus on scaling in pure packet switching, routing, and aggregation as opposed to examining packet load for security threats. It is also possible to introduce a new purpose-built security network element at the edge of the network, but at an additional cost and operational overhead. Additionally, these new network elements potentially may not scale in performance as subscribers and new threats grow.

RG's terminate services like VoIP are evolving to support high-capacity storage devices that enable the RG to function as a home-networked file access server. In the near term, service providers are exploring converged fixed/mobile services. Many of these scenarios require an end-to-end security framework, which suggests that comprehensive security processing is better handled by RGs.

As in the past, security threats will continue to evolve, as will the applications that subscribers demand. Remote configuration capabilities and software download features in standardized remote RG management frameworks can help service providers quickly adjust to changing conditions. For example, when new security threats arise, service providers with a remote management framework can immediately download a new policy, rule set, and signature data to prevent an attack.

Conclusion: Value-Added Next-Gen RGs

Next-generation RGs are changing to support a broad array of new applications. But to ensure that users experience high QoS, a strong security framework is needed to support new applications for the digital home and SOHO/SME market. One technology that is enabling RGs and SOHO/SME gateways to meet the demands of service providers and end-users is DPI. DPI-enabled gateways offer service providers an opportunity to expand their service offerings beyond triple-play services and start offering revenue-enhancing services such as unified threat management services, as well.

This scenario poses a challenge to both system vendors and RG silicon vendors. They must deliver flexible architectures that are not only programmable in nature, but also achieve higher performance when packet payload examination takes place. This requirement essentially drives newer architectures to consider a combined software/hardware model to attain flexibility while not sacrificing performance. With DPI-based security frameworks, silicon vendors can deliver next-generation gateway processors that support unified threat management services and provide an effective toolkit infrastructure to enable faster integration of security software application.

For more information, contact Ikanos.

Ikanos Communications, Inc.
47669 Fremont Boulevard
Fremont, California 94538

www.ikanos.com

P +1 510.979.0400

F +1 510.979.0500

E sales@ikanos.com