The migration of television and video programming to IP comes as a natural progression of technological and market developments. IPTV opens myriad opportunities for service providers to offer new services and increase revenues. IPTV is a key component of service provider multiplay—video, Internet and VoIP services—and opens the doors to create other, more innovative hybrid broadband services (HDTV, for example, or multiplayer gaming). Because IPTV allows service providers to stream only the specific movie or other program requested by subscribers (instead of all content from all channels, as with older, RF-based cable delivery systems), it brings new efficiencies to Multiple Service Operator (MSO) networks. IPTV provides a platform that can easily add interactive capabilities, such as program keyword search engines and picture-within-a-picture reference while channel surfing, making the viewing experience “stickier.” Of course, the rise of video on demand (VOD) results directly from IPTV growth. Combined, these trends help service providers generate higher Average Revenue Per User (ARPU) year after year.

However, IPTV’s growth forces service providers into a double bind—while the demands of video put a premium on network performance, IPTV also exposes video applications to IP security risks. To protect their investments, IPTV service providers need to secure their networks against attacks and incursions, while guaranteeing the high performance that video services demand.

**The Challenge**

The first rule in IPTV services: high performance is the price of entry. Like voice, video content depends upon real-time data transmission, and will suffer—along with customer confidence—if subjected to packet loss or delays.

In this context, then, any attack launched against an IPTV network could spell disaster. A typical IPTV network encompasses numerous critical-path appliances and devices, each of which has its specific vulnerabilities and may become the target of an infiltration. Data servers, such as those that maintain transaction and other details from set-top boxes (STBs) installed in subscribers’ homes, may be hacked by vandals or criminals. Content servers, such as the massive VOD servers that stream video, may also become magnets for cybercriminals and thrill-seekers. Other assets, too, can succumb to acts of fraud, deviousness or even misguided impulsivity. A large-scale attack on these or other strategic service provider assets could anger subscribers, spark a public relations uproar and undermine consumer confidence.

But poorly designed security measures, on the other hand, can themselves cripple performance. While advanced techniques such as stateful firewalls may provide the highest levels of network security, they are wholly inappropriate for screening video packets, since the amount of latency introduced would render video quality unacceptable.
In order to secure their networks, IPTV service providers need comprehensive security solutions that can respond to threats at multiple levels without compromising network performance or service quality. At the very least, the properly designed IPTV security solution needs to address the specific risk profiles and performance requirements associated with each network element, application and subscriber device. Like any other form of security, network security requires multiple measures, in order to apply the appropriate protection at each specific point of vulnerability. Balancing the dual imperatives for high performance and secure operations in IPTV networks requires security solutions that offer multiple techniques in a tiered fashion:

- **Platform Defense:** First-line measures guard hardware platforms and operating systems against malicious broadsides such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
- **Transaction Defense:** Second-line measures protect against more sophisticated incursions by screening for unauthorized data sources or protocol violations.
- **Deep Packet Defense:** The most thorough approach to network security, IPS techniques involve examining the contents of individual packets as a means of validating transactions and data integrity.

Because of their complexity, IPTV networks require security solutions that involve all three of these techniques simultaneously. IPTV security solutions need both a breadth of capabilities and the intelligence to apply each technology judiciously.

**The Juniper Networks® IPTV Security Solution**

With its integrated intrusion prevention system (IPS) capabilities, the ISG2000 combines tiered security with centralized operations, administration and management, and is ideally suited for securing IPTV networks and infrastructures. The ISG2000 is a purpose-built, high-performance security gateway designed to deliver scalable network and application security for large enterprise, service provider and data center networks. Fully integrated with firewall, VPN, and IPS capabilities, the ISG2000 offers multi-gigabit performance, a modular architecture and rich virtualization capabilities.

The ISG2000 tiered security enables service providers to apply the appropriate security measures to each threat category. Its robust firewall and IPS capabilities make the ISG2000 a strong bulwark against attacks on operating systems and hardware platforms. The ISG2000 also protects against protocol violations and data from unauthorized sources through the configuration of policies within the firewall system. What’s more, through the use of protocol signatures, the ISG2000 has the capability to analyze packet structures as a means of screening out unauthorized—and potentially malicious—transactions.

These scalable filtering capabilities on the ISG2000 allow packets to redirect according to their specific risk profiles. The ISG2000 performs a stateful inspection of all data flows to ensure that they conform to accepted rules. Custom signatures loaded onto the ISG Series allow it to determine those packets that require more thorough interrogation. Deployed in an array within an IPTV network, each ISG2000 can be individually configured to determine which packets are intended for middleware applications, and thus need Deep Inspection by IPS blades. The intelligent ISG2000 identifies traffic that is not associated with either middleware or protected applications, and allows these packets to bypass the firewall entirely, thus maximizing its own performance as well as that of other IPTV network elements. These selective security measures help to ensure high performance, and high service quality across the IPTV network.
Features and Benefits

The ISG2000 offers the multi-layered protection, high modularity and advanced capability set demanded by IPTV service platforms. The ISG2000 integrates robust firewall technologies with deep packet inspection capabilities and IPS, along with the intelligence required to inspect and direct packet flows in accordance with their functions and risk profiles. Its firewall capabilities protect hardware platforms and operating systems against DoS, DDoS and other common incursions, while IPS functionality enables high-speed packet inspection as a tool to guard against Layer 4-7 attacks such as zero-day, worms, trojans and spyware. Deep Inspection technologies on the ISG2000 provide protection at the application layer via the use of stateful signatures associated with specific middleware in the network, as well as protocol anomaly detection techniques.

In addition, the Juniper Networks ISG2000 Integrated Security Gateway is a fully integrated firewall/VPN system that supports centralized, policy-based management, for reduced operating expense and flexible deployment. The ISG2000 provides multi-gigabit performance, and scales economically to support up to 10,000 subscribers per chassis. IPTV service providers can deploy the ISG2000 in a variety of configurations to suit their particular service architectures, whether centralized or distributed. Finally, as befits an IPTV security solution, the ISG2000 supports a number of HA configurations, defending servers, service platforms, appliances and other assets from fraud and abuse.

Summary—Juniper Networks ISG2000 Secures IPTV Networks

With millions of subscribers worldwide, IPTV is poised for continued growth. While strategic in its own right, IPTV also provides a baseline offering to which service providers can add other services, all with the goals to expand subscribers, reduce subscriber churn and increase ARPU. With so much riding on IPTV’s success, service providers simply cannot afford to wait until a major attack occurs before bulletproofing their networks. Nor can service providers afford to adopt a simple, monolithic defense mechanism in their quest to achieve both high service quality and high security.

Success in IPTV services demands both high performance and high security. To ensure both, an IPTV network security solution requires a tiered approach that harnesses multiple, advanced technologies to cope with the numerous threats—both current and future—that put network resources at risk. What’s more, an IPTV network security solution needs the intelligence to apply each technology whenever and wherever it’s needed.

The Juniper Networks ISG2000 IPTV security solution combines IPS functionality, stateless and stateful firewall technologies on a single platform. Its highly integrated design offers centralized management, modularity for flexible deployment and scalability, and HA. With its stateful signature and protocol anomaly detection mechanisms, the ISG2000 lends itself to rapid updating, to provide continuous security even through infrastructure upgrades, new service rollouts and even the addition of new service platforms.

Next Steps

No matter what the service mix or delivery model, Juniper’s flexible and scalable IPTV security solution can deploy in a number of centralized or distributed configurations. Contact your Juniper Networks representative for more information about the ISG2000, or about other products that can help you get the most out of your IPTV network.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.