
White Paper

The Top 8 Criteria for Evaluating Multi-Service Security Gateways

Includes Deployment Scenarios and How Juniper Networks Solution
Stacks Up

Written by

Mark Bouchard,
CISSP and Independent Security Consultant

Part Number: 200157-001 October 2005

Executive Summary

The best defense against today's increasingly sophisticated attacks is a layered security solution. Layered security leverages multiple, complementary technologies to protect the network – if one fails to stop an attack, it should still be caught by one of the supporting layers. Increasingly, IT professionals are evaluating devices that combine security technologies that make sense together – beginning with firewall and VPN and now branching out to include intrusion prevention.

Multi-service or integrated security gateways are not a new concept. Numerous products have been on the market for several years now. However, a variety of concerns and cautions (read: limitations) have relegated them predominately to a handful of “low-stress” use-case scenarios. In general the perception, and to a large extent the reality, has been that combining a variety of security services on a single device – while beneficial in terms of the breadth of security functions covered – inevitably compromises in terms of depth of capabilities, manageability, and performance. Nonetheless, these characteristics have proven to be a good fit for situations where economic considerations are dominant and where criticality and performance are less of an issue.

Thus, while a fair degree of success has been achieved for branch office and small/medium business implementations, penetration into high-stress use cases has occurred at a much slower rate. This is not to say that the concept of a multi-service security gateway (MSG) is not applicable in high-end use cases, but rather that the products required time both to mature and to establish a proven track record of being “enterprise class”.

This paper will outline the top 8 criteria to look for when evaluating MSGs and provide scenarios of how and where these solutions can be deployed to provide maximum protection. It will also provide an example of how to effectively consolidate multiple security services by exploring the characteristics of Juniper Networks Integrated Security Gateway (ISG). Indeed, the ISG essentially represents a new sub-class of MSG – one that is purpose-built to meet the higher standards for performance and security that are generally associated with Internet perimeter and data center deployments at large “headquarters” locations.

The Top 8 Criteria for Evaluating Multi-Service Security Gateways

A multi-service security gateway should

1. Provide a set of services that is functionally well aligned.
 2. Provide a set of services that organizations actually need.
 3. Consist of services that are individually best-of-breed.
 4. Enhance security, not compromise it.
 5. Provide adequate performance.
 6. Be highly manageable.
 7. Provide a reasonable savings in terms of cost of ownership.
 8. Provide a high degree of integration.
-

The Top 8 Criteria for Evaluating Multi-Service Security Gateways

In general, for a multi-service security gateway to be a suitable substitute for the common practice of deploying a collection of single-purpose products it must address each of the criteria identified below.

1) A multi-service security gateway should provide a set of services that is functionally well aligned

This has to do with the appropriateness of merging a given set of capabilities into one device, and ultimately determines the practicality of a solution. For example, how useful would it be to have a tool that combined email encryption and web-application firewalling?

Juniper Networks ISG Solution

Additional background on the ISG series products is essential for understanding the response to this criterion, as well as many of the others. In short, the ISG is a purpose-built, ASIC-based security appliance which includes a management module and 2 to 3 (depending on the model) security modules, each with dedicated processing and memory resources. Out of the box the ISG delivers firewall and virtual private network (VPN) services, with intrusion detection and prevention (IDP) being the first flavor of security module to be made available.

Returning to the first criterion, the alignment between firewall and VPN services is well established. After all, it is nearly impossible to find a leading firewall product that does not include integrated VPN capabilities. The appropriateness of combining firewall and IDP is a little more involved, but still rather intuitive. In practice, behind firewalls, IDP products are the most common second/companion device currently deployed by organizations. Not surprisingly, this is because functionally they are highly complementary.

In general, firewalls are intended to limit the flow of traffic to only those communications that are deemed relevant to the business. This inherently reduces the exposure of the enterprise by preventing a vast array of otherwise possible traffic streams from entering its network. However, it typically does not account for the possibility that permitted traffic also includes bad elements, such as viruses, worms, or other sorts of attacks. In addition, many firewalls are limited in terms of visibility and control to operating at the network and transport layers of the communications stack.

This is where intrusion detection and intrusion prevention come into the picture. By conducting a deep examination of all packets that comprise communications traffic, network-based intrusion detection engines can uncover a wide variety of suspicious activities and legitimate threats, including ones operating at the application layer. Associated prevention

capabilities can then be exercised to automatically eliminate the certain threats, while the remaining (suspicious) items can be flagged for closer review, typically by an administrator.

Essentially, IDP picks up where firewall services leave off. They extend protection to the application layer and filter allowed traffic streams to identify and/or prevent suspicious and malicious elements.

2) A multi-service security gateway should provide a set of services that organizations actually need

At first this may sound a bit redundant with criterion #1, but it is actually about accounting for *both* previous security investments that have been made, as well as ones that may be necessary in the future. What it means is that there should be some flexibility in terms of which services get used (and paid for), as opposed to being locked in to a fixed set.

Juniper Networks ISG Solution

Many MSGs offer a fixed set of services with no ability to opt out for ones that are not needed in a given implementation scenario. In contrast, the ISG can be operated as a single service, or any combination of the three that it supports. Furthermore the IDP service is an elective add-on (although “Deep Inspection” technology, a subset of IDP functionality, is built-in to the core firewall) and it can be operated either in passive or in-line modes, with the ability to switch between the two without having to change the network configuration. Finally, the ISG’s architecture makes the service portfolio completely extensible. Future security flavors of security module are inevitable, and could easily include services such as anti-virus, or even session border controllers to accommodate the growing need to secure VoIP traffic.

3) A multi-service security gateway should consist of services that are individually best-of-breed

Compromising when it comes to effectiveness will ultimately undermine the expected benefits of using an MSG (e.g., cost savings).

Juniper Networks ISG Solution

Individually, the Juniper Firewall/VPN and IDP services are widely recognized to be among the market leaders in their respective classifications. In adapting these services to the ISG there has been essentially no feature/function fall-off. In contrast, many MSGs seek to establish the broadest possible set of security services, and in doing so extend beyond the core strengths of the parent vendor. Clearly, there are scenarios where such a compromise may be acceptable, but in general it is sensible to stick with best-of-breed as much as possible.

4) A multi-service security gateway should enhance security, not compromise it

Security improvements should not only be inherent (i.e., on the basis of having multiple security services) but should ideally also stem from integration between services enabling the whole to be greater than the sum of the parts. In terms of potential avenues of compromise, the design should be such that failures in an individual service do not enable other services to be bypassed.

Juniper Networks ISG Solution

The best-of-breed discourse, the discussion on IDP being complementary to FW/VPN, and pending discussions on integration and virtualization apply here as well. In short, security features are intertwined with and pervade virtually all other aspects of the ISG. Nonetheless, some additional highlights include the following:

- IDP has a substantial set of signatures that apply to the server-to-client direction of traffic flow, giving it a uniquely deep, bi-directional protection capability.
- Sharing and correlation of events between the services enables greater accuracy when it comes to separating legitimate threats from merely unusual activities. In addition, the firewall's policies can be used as yet another enforcement mechanism at the disposal of the IDP.
- ScreenOS is a purpose-built, hardened operating system that is not subject to vulnerabilities common to general purpose operating systems.
- FW/VPN and IDP are not fully interleaved (i.e., they are not a single blob of code), thereby reducing the possibility for vulnerabilities in one service to adversely impact another.

5) A multi-service security gateway should provide adequate performance

Even with all services operating under real-world traffic conditions it should be possible to maintain reasonable throughput levels. Ideally, the device/system architecture should exhibit performance-enhancing characteristics while configuration options should be available to selectively reduce the impact of known, performance-sapping services.

Juniper Networks ISG Solution

The ISG was purpose-built to accommodate multiple security services, as opposed to many other products which appear to have grown into MSG status by just lumping more services onto an existing device. This applies both to the hardware as well as in terms of the interoperability of the services.

The core ASIC module provides intelligent, accelerated packet processing and includes a set of programmable processors to accommodate future upgrades with minimal impact. In

addition, each of the other modules includes dual, high-speed processors and dedicated memory, while the security modules also employ an FPGA, in this case to accelerate signature lookup for the IDP service.

The “intelligence” aspect is also significant because it ensures optimal use of the management and security modules by only sending packets to them as needed. For example, the system would know not to send the media stream of an IP telephony session to the IDP, since there are no signatures/inspection applicable to this sort of traffic. Furthermore, administrators have the option to manually configure which traffic streams should be subjected to IDP, and subsequently to which specific inspections within IDP’s arsenal.

In aggregate these features enable the ISG to utilize highly intensive inspection techniques (e.g., stream re-assembly, server-to-client), reaching a higher degree of security without compromising in terms of performance. Significantly, this also affords organizations the luxury of not having to worry about the specific types of applications that are running in their environment. Increasing use of small-packet and latency sensitive applications (e.g., VoIP, multi-media) is handled gracefully and without incident. Policy decisions are made and executed with no delay while performance remains consistent regardless of packet size.

6) A multi-service security gateway should be highly manageable

It should not be necessary to operate multiple management applications.

Juniper Networks ISG Solution

The NetScreen Security Manager is available as a single management console for all ISG capabilities, though many features are also optionally manageable via command line interface or a web UI. With the exception of policy configuration, the majority of the management capabilities are shared between the different services (e.g., logging, alerting, and reporting). However, even while policies are maintained separately, there is standardization in terms of rule format as well as direct linkages between them. For example, the firewall policy, which is processed first, includes a rule attribute that designates whether associated traffic should be subject to further inspection. The IDP policy then covers the particulars of that inspection.

Also critical for an MSG is the ability to optionally maintain separation of duties, an important management principle that ensures against practices such as sweeping alerts “under the rug” by re-setting the policy to keep them from triggering in the first place. The NetScreen Security Manager easily meets this objective, supporting highly granular assignment of administrative responsibilities, both in terms of functions as well as by various grouping constructs.

Of course, it is important for organizations to realize that “highly manageable” is not the same as requiring no/minimal administrative effort. Taking full advantage of the ISG’s security capabilities requires delving into numerous application layer details, and configuring

associated inspections to account for the unique characteristics of an organization's environment inescapably involves a certain degree of complexity.

7) A multi-service security gateway should provide a reasonable savings in terms of cost of ownership (e.g., 30% or greater)

This is necessary to account for disruption and change-out costs and to ensure further benefit is realized relative to employing an approach dependent on standalone products.

Juniper Networks ISG Solution

Reductions in the number of separate security devices and management applications, network complexity, vendor management, deployment effort, and operator training are all intuitively realistic benefits of an MSG and can yield some measure of cost savings. Of course, the ISG goes beyond this. For instance, deployment is further simplified relative to other MSGs based on supporting multiple implementation modes (e.g., transparent, routing, or NAT) and in general by being highly network-aware. In addition, a high degree of integration unlocks hard-to-quantify operational benefits in the form of greater efficiency and automation. However, an equally significant point is that compared to other MSGs which purport to deliver many of the same cost savings, the ISG does so without having to cut corners in terms of either performance or depth of security.

8) Speaking of a “high degree of integration”, that characteristic has purposefully been left to last, but is far from being least in terms of its importance

Juniper Networks ISG Solution

By necessity, many aspects of this criterion have already been discussed. This is because the degree of integration underpins many of the other items listed here, particularly security, performance, manageability, and the potential for cost savings. Indeed, without a high degree of integration, there would be little benefit to using an MSG as opposed to a collection of best-of-breed point products. Accordingly, by design the ISG emphasizes integration.

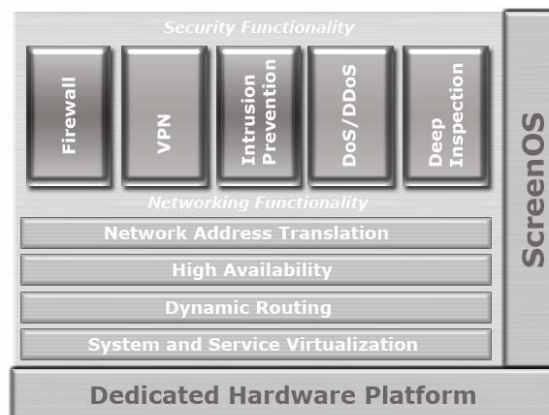


Fig 1. Juniper Networks ISG: An Architecture Emphasizing Integration

At a high-level, the standalone IDP was not simply bolted on to the existing FW/VPN solution. Instead it was significantly revised to have its policy and management functions be absorbed into the ISG's management module and to take advantage of initial packet processing and network-level services available as part of ScreenOS and the associated ASIC module. Similarly, all of the components of the ISG were revised to account for the internal "workflow" necessitated by such a division of labor.

The resulting design could be characterized as "integrated yet separate", and is the root of many of the benefits that have already been identified. For example, strategic separation enables selectivity with regard to which services are operated, low susceptibility to cut-through vulnerabilities, and functional specialization. On the other hand, integration facilitates improved threat detection accuracy and response times and more efficient operational process (e.g., policy management, troubleshooting and forensics).

Deploying Multi-Service Security Gateways within the Network Infrastructure

The ISG is relatively unique with regard to the extent that it simultaneously fulfills all of the above criteria. In contrast, alternative MSG designs tend to focus on a handful of these items, while compromising on others. For example, chassis-based products often achieve high performance levels for one or a few security services, but commonly lack high degrees of integration and manageability. Similarly, branch-office MSGs based on less-specialized hardware and smaller form factors often emphasize breadth of security services covered and a lower price point in favor of performance and depth/quality of the services that are included.

Nonetheless, this does not mean that the ISG is appropriate for all use cases. Indeed, the smaller MSGs just described will typically be the right choice for small/medium enterprises, as well as for the branch offices of larger enterprises. They strike an ideal balance between cost and capabilities for these lower stress use cases. On the other hand, standalone, single-service products will still be appropriate for very high-end use cases, that is, those requiring maximum performance/capacity levels and/or specialized functionality. Overall, this leaves products like the ISG best positioned to address the intermediate scenarios, from a capacity and criticality perspective.

Of course, there will inevitably be overlap in terms of how the products in these three loosely defined categories are employed. Different organizations will weigh the tradeoffs between the different approaches differently. No matter. At least they have a choice. In addition, due to the strengths of the ISG it can be expected to encroach on the standalone products being used in high-end scenarios, at least for the services that it covers. Indeed, for many enterprises the ISG should be suitable for implementation at the Internet perimeter, on the internal network, and even within the data center.

DMZ

Discussions of a so-called dissolving perimeter can be misleading. The intent is to convey that defending the Internet perimeter is insufficient given the other avenues that communications traffic may take, particularly as a result of various mobility and inter-connectivity technologies that are being widely adopted. The intent, however, is not to convey that the Internet perimeter itself is going away, or that the practice of defending it should be abated (at least not yet). Internet DMZs are still relevant, and will be for some time – at least until internal and host-based safeguards are made pervasive (and even beyond that, assuming the principle of defense-in-depth continues to be practiced).

In fact, security at Internet perimeters should continue to be bolstered, not diminished. Adding intrusion detection and prevention capabilities – and more broadly, protection against application layer attacks – to existing perimeter safeguards is definitely appropriate. As already discussed, these are mechanisms that are both necessary and complementary to commonly deployed controls such as firewall and anti-virus gateways. Another key point is that the DMZ environment, in being a bridge between relatively low-speed Internet links and relatively high-speed internal networks, typically involves intermediate capacity (though potentially strenuous latency and jitter) requirements. In aggregate, these requirements clearly represent an ideal use case for the ISG with IDP, which would be a good fit at the Internet perimeter both economically and functionally.

Dividing Domains

Rightly so, much has been made in the past 2 years about the need to secure internal networks. Numerous paths around perimeter defenses, not to mention a plethora of threats which inherently reside ‘on the inside’, must be acknowledged and subsequently addressed. Logic aside, it is also the case that a variety of legislation effectively dictates that organizations must deal with this issue.

In doing so, the key point that organizations must realize is that internal networks are typically more complicated than perimeter networks. This is a result of internal networks having a greater variety and volume of moving parts. There are substantially more hosts to protect, more protocols and applications to understand, more users/roles to distinguish, and a much greater rate and volume of traffic.

Fortunately, once again the ISG is well positioned to meet these needs. Not only does its architecture ensure adequate performance in this highly intensive use case, but it also includes the following beneficial features:

- Support for virtual systems. This is the ability to specify multiple, separate firewall inspection policies (i.e., virtual firewalls) or routing policies (i.e., virtual routers).
-

- Support for virtual LANs. This is the ability to treat traffic from different physical or virtual ports as belonging to the same communications domain.
- Support for security zones. Logically similar to VLANs, this is another layer of virtualization that enables grouping of traffic from diverse interfaces under a single security policy.
- Support for multiple deployment modes (i.e., transparent, routing, or NAT).

Ultimately this enables highly flexible segmentation and isolation of internal traffic that belongs to different trust levels (i.e., has different security needs) or different functional/business units. In other words, it means being able to apply and enforce the right policies to all traffic streams, even in highly complex environments, and without significant impact on the network itself.

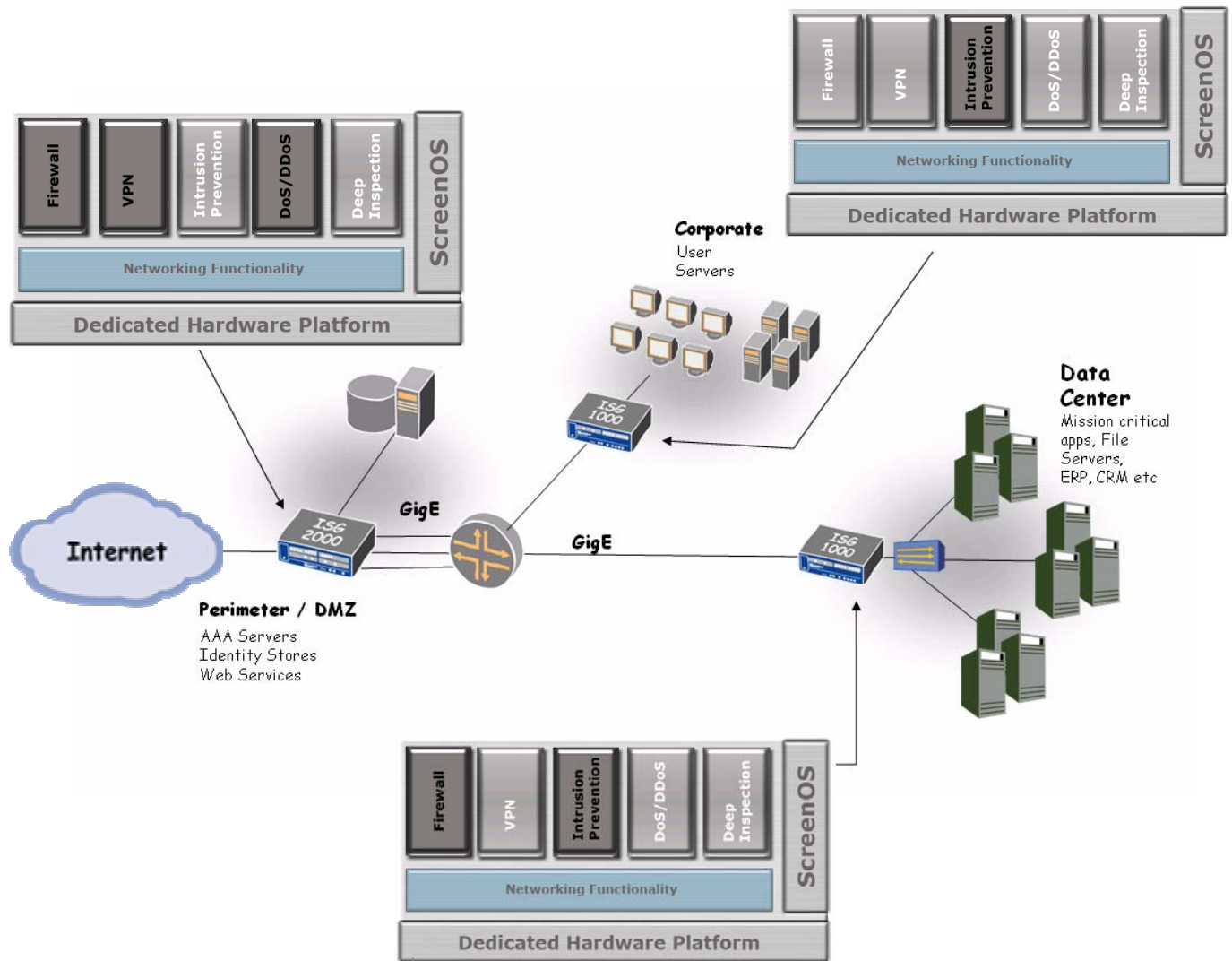


Fig. 2 Multi-service security gateways allow for flexible deployment options – with the choice of enabling some or all security functionality to match the network and protection requirements

Data Center

Obviously the data center is part of the internal network as well, and as such it exhibits many of the same characteristics and derivative requirements. However, it is set apart here to recognize that, typically, it is an even more intensive use case than that of providing secure segmentation of internal domains. The scale of operations and underlying performance and criticality requirements can easily be an order of magnitude beyond that of other areas in the internal network. As such, this becomes one of the specific implementation scenarios where use of standalone devices may prove necessary. Still, the ISG will hold its own for many enterprises, even offering a few benefits (beyond those listed above) for those cases where its performance/capacity are sufficient:

- Denial-of-service attack protection capabilities.
- Broad, open, and extensible attack coverage. Protection can be provided for additional services and applications (including home-grown ones that inevitably reside in most data centers) simply by customizing existing attack signatures or adding altogether newly created ones.
- Native support for multiple high-availability modes (e.g., active-passive, active-active, and active-active ‘full mesh’, which includes the ability to monitor the state of other upstream/downstream devices and failover accordingly).

Summary

Juniper’s ISG with IDP clearly addresses the historical cautions which have now come to represent the key criteria for establishing the suitability of a multi-services security gateway. In addition, its high degree of integration and intelligence, including awareness at the application layer, are instrumental in enabling it to facilitate automated response to legitimate threats. Furthermore, its architecture and associated flexibility make it suitable for use throughout the enterprise computing environment.

The result is a solution that simultaneously meets the dual objectives of being highly effective and highly efficient. From a technical perspective this means getting predictable performance without having to compromise in terms of security. And from a financial perspective it simply means lower cost of ownership. The bottom line: ISG with IDP is a solution that actually stops more threats with fewer components while costing less.

About the Author

Mark Bouchard, CISSP, is an independent consultant focused on information security and risk management strategies. A former industry analyst with the META Group, Mark has assessed and projected the business and technology trends pertaining to a wide range of information security topics for nearly 10 years. He has established a reputation for thought leadership and is a sought after speaker in the areas of security architecture, DMZ design, secure remote access, network security, and related technologies (e.g., firewalls, intrusion prevention systems, and virtual private networking).

He is passionate about helping enterprises address their information security challenges. During his career he has assisted hundreds of organizations world-wide with everything from strategic initiatives (e.g., creating 5 year security plans and over-arching security architectures) to tactical decisions involving the justification, selection, acquisition, implementation and ongoing operations of individual technologies/products. In addition, he routinely works intimately with the creators and sellers of information security solutions, helping them to better understand and meet the needs of the market at large.
