Whitepaper

Juniper Networks Firewall/VPN Buyers Guide

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 710008-002 Oct 2006

Contents

Introduction

Technology is radically changing the way companies conduct business, opening up new possibilities that enable efficiencies and growth on a global scale. But for everything that technology facilitates, it also opens up new risks, forcing companies to think about how to protect the assets they are working so hard to build. Security and IT administrators are faced daily with the challenge of successfully implementing technology that supports the company's success, while maintaining the security of the organization's critical resources.

The first task that organizations use a firewall for is to control who and what gets in and out of the network. Initially deployed at the perimeter, firewalls perform a myriad of services based primarily on IP addresses and source/destination ports, including basic access control, user authentication and policy enforcement to ensure only appropriate users and services are able to traverse the network. When evaluating today's firewall offerings, it is critical that corporations also look at ways to augment or replace the firewall based access control with an offering that grants/denies access based on more granular criteria including end-point state and user identity in order to accommodate the dramatic shifts in attack landscape and user characteristics. Regardless of the access control methodology implemented, one fact is clear, firewalls are no longer relegated to just perimeter deployments.

Rather organizations are increasingly taking advantage of firewall capabilities throughout the network to segment it and apply security policies such as access control, IPSec VPN, and attack protection between different segments. These segments, or zones, could represent geographically distributed networks, such as regional offices, different types of traffic, such as wireless or VPN connections, different departments or even different servers. This segmentation enables the organization to create additional levels of trust to protect sensitive resources and perform attack containment.

Firewalls also provide some protection against attacks, traditionally focusing on preventing network-level exploits, such as Denial of Service attacks. But, as many organizations have come to realize, the attack landscape is continually changing to where protection is required not only at the network layer, but also at the application layer and the content or payload layer. Making matters worse is the need to monitor and filter both inbound and outbound traffic to deliver protection against internal attacks and malicious employees as well as the traditional, external attacks. As a result, many firewalls have started to look deeper into the traffic at multiple levels (network, application and content) they are allowing in and out of the network to try to identify and prevent attacks before the inflict any damages.

Firewalls are also often coupled with virtual private network (VPN) functionality, which is designed to enable organizations to provision site-to-site connectivity that takes advantage of the cost-benefits of the public Internet infrastructure in a secure manner. The most commonly deployed site-to-site VPN technology is an IPSec VPN, so this guide will focus on these solutions. IPSec VPNs encrypt traffic to maintain its confidentiality and protect against tampering with or altering of the data. As a result, they enable organizations to securely extend their network perimeter across the public Internet to facilitate secure communications between geographically distributed locations.

As with any solution, an administrator needs to be aware of the potential impact that a device can have on their network's performance and availability, as well as the time and management implications that each solution introduces. While VPN functionality can also be deployed as a standalone solution, it is always a good idea to apply access controls to the VPN traffic. As a result, the tight integration of firewall and VPN functionality can reduce network complexity, simplify deployment and management and reduce the overall total cost of ownership of an organization's connectivity and security.

Administrators need these solutions to enable business productivity, as well as network security, so this guide is designed to help organizations find the balance they need between functionality and security, without compromising one for the other. This guide provides a framework for evaluating firewall and VPN security solutions. It is organized into three sections. The first is an executive level summary that splits the evaluation criteria into five different categories and explains the impact of each category on the overall solution's ability to deliver value. The next section takes those five categories and provides a quick checklist for each that will help the evaluator start to ask the questions that will differentiate the capabilities of products. Finally, the last section provides a detailed list of features that make up each category to enable evaluators to really make product comparisons to ensure they can select the one that best meets the needs and requirements of their organization.

Executive Summary

Firewalls serve as the foundation upon which a strong network security solution can be built, so the purchase decision should be framed in terms that support a long-term investment to support the organization's needs as they change and grow. The chosen firewall/VPN solution should not only provide robust security functionality, but also the networking and availability features that will support the company's ongoing connectivity and expansion requirements. In addition, the security solution needs to be easily integrated into the network and simple to manage, so that it does not pace additional strain on the already tight IT, security and networking budgets. There are so many firewall and VPN vendors in the market that it can become overwhelming for a company to try and sort through them all and determine what the best solution is for their environment. This section is designed to help decision-makers and evaluators think, in broad terms, about the criteria that will be most helpful as they make their security solution choice.

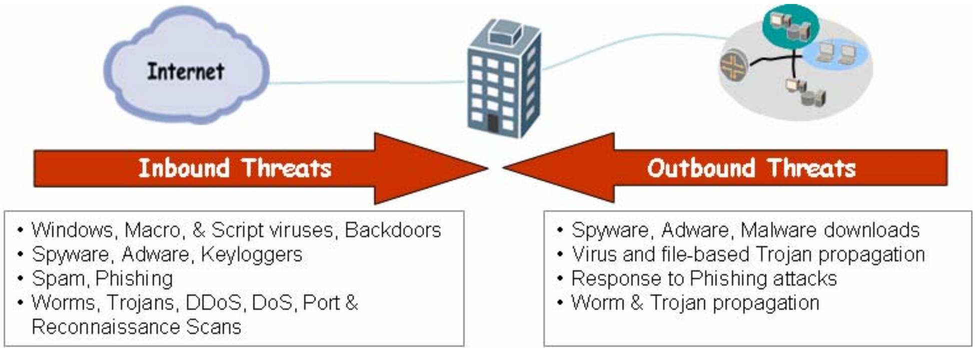
Provide Strong Security

The solution needs to provide robust security functionality to maximize the protection it provides to the network. Some of the functionality that should be supported includes strong access control, and user authentication using either the firewall and/or one that uses more granular criteria including end-point state and user identity to grant/deny access in order to accommodate the dramatic shifts in attack landscape and user characteristics. In addition to control who and what gets into the network, multi-level attack protection, IPSec and encryption choices for data integrity, and network segmentation for attack containment are critical features to look for in a firewall.

Solutions too simplistic in their approach, while initially appealing because they seem to be easy to manage, actually end up creating more work because of the holes they end up creating that can be exploited to attack the network. For example, how effective is it to add access lists to a router if they do not track the state of the communication, perform Stateful Inspection of protocols, look for and block all manner of malware, or offer strong authentication, leaving the network vulnerable to potential unauthorized use? In response, it is important that the solution provides the granularity and flexibility needed to identify differences in traffic and appropriately process that traffic. Ideally, the functionality should be integrated to maximize the security derived from the solution. Integrating the VPN functionality into the firewall, for instance, requires fewer open ports and enables firewall policies to be easily applied to VPN traffic. In addition, it is important to identify potential vulnerabilities that could be introduced by the device itself, such as those associated with general-purpose platforms and operating systems. It is also important that the solution accommodate the different requirements of different network segments, from the smallest remote office to the largest central site, to ensure security can be uniformly deployed and eliminate any weak links.

Best-in-Class Attack Protection Against Malware

As the network attack landscape continues to evolve, IT managers can no longer afford to focus solely on protection against a single type of attack and expect their network to remain unaffected. All manner of attacks are pointed squarely at the corporate network. Relatively simple network level attacks have morphed into more complex attacks that use both network and application level components to achieve their malicious goal. With more and more companies providing direct access to the web, end-users are casually surfing to sites that may be known malware download sources, or unknowingly revealing personal or corporate private data (credit cards, passwords, corporate trade secrets, etc) via email scams or hidden background programs that collect and forward data. This means IT manager must look at ways to stop inbound and outbound attacks at the network, application and content layers.


Internet
Inbound Threats
Outbound Threats
• Windows, Macro, & Script viruses, Backdoors
• Spyware, Adware, Keyloggers
• Spam, Phishing
• Worms, Trojans, DDoS, DoS, Port & Reconnaissance Scans
• Spyware, Adware, Malware downloads
• Virus and file-based Trojan propagation
• Response to Phishing attacks
• Worm & Trojan propagation

- Inbound threats are those that originate from outside the corporate network, for example, from an attacker on the Internet who intends to penetrate the corporation's perimeter defenses. These threats include virtually all manner of attacks from worms to viruses to Spyware to Phishing emails.
- Outbound threats are those that originate from someone sitting inside the corporate network, such as an employee sitting in their cube who has a machine that has been unknowingly compromised and is propagating a worm or virus throughout the corporate network. Other examples of outbound attacks are users who respond to Phishing attacks by entering their personal data on a malicious web site, and Spyware sitting on an employee's machine quietly sending sensitive corporate information to some malicious party on the Internet.

Stopping inbound and outbound attacks requires a concerted, multi-layered solution to prevent them from inflicting damages on network assets and the end user.

Offer Predictable Performance

Regardless of where the FW is deployed, be it a datacenter, a perimeter, or a branch office, the FW needs to be an enabler to network connectivity rather than a barrier. If the solution cannot keep up with the performance requirements of the network location it is designed to protect, its value will be significantly diminished. Not surprisingly, it must be able to efficiently process traffic and deliver predictable performance under load. The performance should be sustainable for both large and small packets. It should also minimize latency and accommodate the necessary concurrent sessions and VPN tunnels that are required for that particular network segment. In order to provide adequate Denial of Service (DoS) protection the solution needs to support a high ramp rate to handle attempts at performance overload. The solution must be able to handle the performance requirements of the network and function without degradation as security features are enabled.

Facilitate Branch Office Device Consolidation

Industry research shows that the number of employees located outside of headquarters is upwards of 80%, a fact supported by the increase in the number of branch offices, up 6.5% annually. The reasons are simple. Employers want the best for their employees and providing work environments close to where they live, that are easy to get to and are affordable can only be beneficial in the long run. At the same time, low cost bandwidth and a desire to improve productivity is leading to the deployment of direct Internet connections to branch offices, replacing or augmenting branch-to-corporate backhaul connections. With direct access at the branch comes added security and networking requirements, pushing the average number of network devices in each branch office to seven.

When looking at security and networking devices for the branch office, the ideal solution should give organizations the option of deploying a stand alone security or routing device or a consolidated security and routing device as a means to reduce capital and operating expenses. In order to accomplish this objective, the device must be a security platform first and foremost, capable of supporting a variety of core networking capabilities. Multiple interfaces along with VLANs, useful for security purposes, will need to be accompanied by *proven implementations* of a variety of modular LAN/WAN interface cards to keep pace with future connectivity options along with appropriate routing protocols and WAN encapsulations.

Deliver Fault Tolerance to Ensure Solution Availability

Being able to survive a failure and maintain both connectivity and the security stance of the organization is the sign of good solution. The solution needs to provide redundancy at all levels to give an organization the flexibility to choose the level of availability they want for each of their network segments, based on their cost and connectivity requirements. The device, itself, needs to offer solid-state performance and component redundancy. It then needs to support a high availability configuration that is able to maintain session and state information for BOTH FW and VPN while surviving a failure both up and down stream of the device, via an active/active, full mesh architecture. It needs to include network redundancy, leveraging the resiliency of dynamic routing and supporting path redundancy to multiple ISPs or a dial-back up line. At the VPN level, it needs to support multiple tunnels and minimize failover time to ensure optimal connectivity. Only a solution that is able to provide all of the redundancy pieces is truly fault tolerant.

Offer Ease Of Use And Management

The real costs of a solution are tied not to the initial capital outlay, but to the ongoing management and operational costs associated with keeping the solution up and running. If a solution requires a lot of time and resources to maintain, it is going to take away from other activities and increase the management burden on the organization. The solution needs to be easy to interact with to ensure changes can be quickly made to keep the security policy in force. It should automate as much as possible to minimize human intervention. It should be easy to troubleshoot to enable organizations to quickly resolve problems and it should offer a broad array of support options to ensure problems or questions are handled in a timely fashion. Organizations don't want to waste a lot of time on managing, rather they want an easy to use solution that enables them to spend time on activities core to their business success.

Enable Quick And Simple Deployment And Installation

IT, network and security managers are expected to do more with less, so it is important to be able to get solutions up and running quickly. The solution of choice needs to seamlessly integrate into the network environment, without introducing interoperability issues. It should be intuitive, so that it doesn't require a lot of training or security expertise to use. Updates need to be easy to accomplish, without having to worry about overriding custom configurations or introducing new vulnerabilities. For instance, an organization doesn't want to have to worry about how a newly applied patch to the operating system will affect the underlying platform or the applications that it is running. The solution should be designed with everything working together, to minimize complexity and simplify deployment and installation.

Questions To Ask The Vendors

This section builds upon the framework for evaluating firewall and VPN products that was described in the previous section, providing a quick checklist of some of the top questions to pose in each criteria category. For more in-depth questions that enable a side-by-side comparison of different solutions, go to the Detailed Buyer's Checklist that follows this section.

Strong Security

a. Is it a Stateful Inspection firewall?

b. What types of access control, user authentication and verification supported?

c. How does the offering leverage existing user repositories for access control, user authentication and verification?

d. Can the firewall support, either stand alone, or in conjunction with another solution element, more intelligent forms of access control based upon user identity, endpoint security state and network information?

e. Can the firewall interact with 802.1X-based Layer 2 admission control offerings?

f. What types attacks can the firewall protect against (Network-, application-, content-level)?

g. Are mainstream VoIP protocols supported?

h. Can the firewall protect VoIP protocols without degrading call quality?

i. Will VoIP continue to operate at an acceptable quality level when basic security such as NAT is enabled?

j. Can the IPSec VPN interoperate with other VPNs?

k. What kind of encryption does the VPN support?

l. What type of security certifications does the product have?

m. How does the solution perform attack containment?

n. Is the firewall and VPN integrated-managed from a single console, sharing information, providing the ability to apply firewall policy to VPN traffic?

o. How does the system protect against potential vulnerabilities within the system itself?

p. How does the solution scale to meet the different security needs of small to large sites?

Unified Threat Management Features

a. Are the Unified Threat Management (UTM) features developed in house, or are they leveraging best-in-class attack research and support organizations?

b. Is protection against Phishing, Spyware, Grayware and other malware included as part of the standard AV offering?

c. Is the AV solution a true file-based offering that deconstructs the payload, decodes the file or script, evaluates it for potential viruses and then reconstructs it, sending it on its way?

d. Is the response to virus outbreaks measured in a matter of hours?

e. Does the IPS fully understand the details of each protocol using a combination of methods such as stateful signatures, protocol anomaly detection and other heuristics to stop threats?

f. Does the IPS look deep into the traffic, reassembling it to send it on its way, or does it merely perform rudimentary pattern matching?

g. Does the IPS offering provide multiple response mechanisms?

h. Does the IPS offering provide multiple administrative notification mechanisms?

i. Is the anti-spam target list derived from real-world traffic conditions?

j. How many servers are used to monitor traffic and are they deployed internationally?

k. How often is the anti-spam list updated?

l. How often is the URL filtering database updated?

m. Are there sufficient categories to develop granular web filtering policies?

n. Are there options for either integrated or redirect URL filtering?

Predictable Performance

a. What are the performance (large and small packet size) capabilities of the solution to ensure that performance remains predictable?

b. What has the solution done to optimize its traffic processing?

c. How does the solution handle very fast session ramp rates to protect against DoS attacks?

d. How does the architecture of the solution enable performance under load?

e. How does the solution handle multiple concurrent sessions to ensure user connectivity is not lost or slowed?

f. How does the solution accommodate additional functionality, without degrading performance?

g. How does the solution accelerate the VPN negotiation to set up the VPN tunnels to make the time imperceptible to the user?

h. How does the solution minimize latency to ensure real-time applications are not degraded (e.g. VoIP)?

i. How can the solution quickly create and then maintain VPN tunnels to ensure they are always available for the user?

Device Consolidation

a. Is the device capable of acting as a FW/VPN security device first and foremost?

b. Is the routing engine proven to handle traditional branch office routing requirements?

c. Is performance maintained when security + routing are enabled?

d. Has true WAN connectivity (ADSL, T1, E1, ISDN, DS3, etc) been integrated into the device?

e. Is the LAN and WAN I/O support modular to accommodate future connectivity changes?

f. Are LAN/WAN connectivity options supported by appropriate routing protocols and encapsulations?

Fault Tolerance

a. Does the solution support high availability (HA) configurations, including active/active, full mesh, to reduce the chance of a single point of failure?

b. Does the HA solution maintain both session and VPN state information to ensure that both the connection and VPN security association are maintained in the event of a failure?

c. Can the solution take advantage of dynamic routing as part of VPN resiliency?

d. Can the solution support redundant paths? If so, what kind – multiple ISPs, dial back-up?

e. What redundancy features have been built into the VPN configuration?

f. What are the mechanisms used to minimize fail-over latency and ensure maximum uptime?

Deployment and Installation

a. Is the solution delivered as an appliance for easy deployment?

b. Are there different options that accommodate administrator preferences for installing and configuring the system?

c. Does the solution support CLI, WebUI and policy-based configuration?

d. How easy is it to install a new policy?

e. What networking features does the solution support to facilitate a timely deployment?

f. How are patches applied?

Ease of Use and Management

a. How easy is it to perform management tasks?

b. How quickly can changes be made in a large distributed network?

c. Are there multiple ways to interact and manage the system?

d. How much manual intervention is needed when a connection goes down?

e. How easy is it to troubleshoot problems?

f. How easy is it to add a network to the VPN?

g. How easy is it to configure complex VPN configurations, such as a hybrid full-mesh and hub and spoke?

h. Can firewall policies be easily applied to VPN traffic, without a lot of additional configuration?

i. Is there a broad array of support options?

j. How complex is the support infrastructure? Do you have to deal with multiple licenses or vendors?

Detailed Buyer's Checklist

This section provides a feature/functionality checklist for each of the criteria categories to help evaluators determine the true capabilities of vendor solutions they are considering.

Evaluation Date: ____

Evaluated By: ____

Feature	Juniper Networks Firewall/VPN Solutions	Alternate Solution:	Notes
Strong Security			
Access control and user authentication	Yes		
• User name/Password	Yes		
• Internal Database	Yes		
• RADIUS	Yes		
• LDAP	Yes		
• SecureID	Yes		
• Xauth	Yes		
• Web Auth	Yes		
• X.509 certificates	Yes		
• Tokens	Yes		
• 802.1X	Yes		
Enforce access control policies based upon user identity, endpoint security state and network information	Yes		FWs, working in conjunction with the Infranet Controller (UAC) act as policy enforcement points.
Ability to <u>segment network</u> and enforce policies between segments for attack containment and additional layers of trust	Yes		Using Security Zones, virtual LANs and virtual routers
• Ability to split network into <u>completely separate domains</u> and create security policies for each one	Yes		Using Virtual Systems
• Completely separate policies	Yes		
• Completely separate administrative controls	Yes		
Performs Stateful Inspection	Yes		
Protects against network- level attacks	Yes		
Protects against DoS and DDoS attacks	Yes		
Protects against transport layer attacks	Yes		
Protects against application-layer	Yes		

attacks			
Uses Stateful signatures for attack detection	Yes		
Uses protocol enforcement for attack detection	Yes		
Protects against transport layer attacks	Yes		e.g. Port scans, Tear Drop attack
Protects against network layer attacks	Yes		e.g. IP fragmentation, ICMP “ping of death”
Blocks malicious URLs	Yes		matches user defined patterns
Inspects and protects VoIP	Yes		
• SIP	Yes		
• H.323	Yes		
• SCCP	Yes		
• MGCP	Yes		
• NAT for all VoIP protocols	Yes		
• VoIP specific DoS protections	Yes		
• Security will not degrade VoIP call quality	Yes		
Security Certifications:			
• Common Criteria	Yes		
• ICSA certification	Yes		
UTM Specific			
Block inbound and outbound attacks	Yes		AV = Both inbound and outbound Anti-Spam = Inbound only IPS = Both inbound and outbound Web filtering = Inbound only
All UTM features present consistent management interface	Yes		Some vendors, like Cisco in the ASA use Trend Micro management interfaces to control AV
Best-in-class AV	Yes		Kaspersky AV engine, consistently rated #1 in catch rates, is integrated into the Branch office product line. See appendix A for platform support.
• Anti-Phishing included in AV	Yes		
• Anti-Spyware included in AV	Yes		
• Anti-Adware included in AV	Yes		
• AV Signature DB is updated frequently	Yes		Updates occur every hour by Kaspersky
• AV outbreak responsiveness is less than 3 hours	Yes		Average 1.5 hours by Kaspersky
Best-in-class Anti-Spam	Yes		Anti-Spam engine, developed and backed Symantec technology is integrated into the Branch office product line. See appendix A for platform support.
• Block known spammers and phishers	Yes		Integrated Anti-SPAM is available on a wide range of platforms. See appendix A.
• SPAM list is updated regularly	Yes		Updates are performed as frequently as four times per hour
• SPAM list is generated by worldwide network of millions of honeypots	Yes		Anti-Spam list is generated by Symantec from approximately 3 million honeypots across more than 25 different countries. Approximately 20-25% of all global email traffic is analyzed to generate the Anti-Spam list.
Best-in-class Web Filtering	Yes		Web filtering from SurfControl, consistently rated #1 or #2 in the market, is integrated into the Branch office product line. See

			appendix A for platform support.
• Block access to known malicious download sites or other inappropriate web content	Yes		URL database of over 19 million (30% are international) covering over 2.5 billion web pages across 54+ categories with over 50,000 added every week.
• White list (explicitly allowed URLs)	Yes		
• Black list (explicitly blocked URLs)	Yes		
• User definable URL categories	Yes		
• Assign group profiles for different levels of web access	Yes		
• Use FW authentication for additional level of web access control	Yes		
• Web filtering options: integrated or re-direct	Yes		Multiple options (integrated with SurfControl, redirect with SurfControl or WebSense) provide flexibility and control. See appendix A for platform support.
Strong Security - VPN Specific			
Uses IPSec for secure communications	Yes		Also enables interoperability with other IPSec VPNs
Supports IKE for flexible encryption negotiations	Yes		An interoperability feature
• AES	Yes		
• DES	Yes		
• 3DES	Yes		
Certifications:			
• FIPS 140-1 or 140-2	Yes		
• ICSA IPSec	Yes		
Integrated Firewall and VPN			
FW/VPN managed with the same console	Yes		Simplifies deployment, reduces chance for human error that could result in vulnerabilities
The number of years the solutions have been available on the market	FW/VPN – June 1998 Deep Inspection/Intrusion Prevention – Feb 2002		
The applications that have been recognized as best-of-breed	Yes		FW/VPN/Deep Inspection (Gartner Magic Quadrant)
Firewall policies applied to VPN traffic don't open holes in the firewall	Yes		
Ability to maintain the VPN abstraction and continue to leverage dynamic routing when applying the firewall policy	Yes,		Using Security Zones, Virtual LANs and virtual routers. If the firewall policy requires the use of IP addresses, like some competitive offerings, then the management advantages of dynamic routing are lost.
Built in features that protect against tampering:	Yes		
• Packaging sealed with custom tape	Yes		
• Uses tamper seals to indicate authenticity	Yes		

• Hardware can restrict remote access via access lists	Yes		
• Access list creation based on IP and MAC addresses	Yes		
• Hardware protects against password overrides	Yes		
• Hardware uses secure connections for remote access	Yes		
• Custom OS built for security	Yes		A custom OS is less prone to known attacks than a general purpose OS
• FIPs certified for physical protection of keys and configuration, as well as software protection	Yes		
Guards against vulnerabilities within the system itself:			
• Purpose-built device	Yes		Purpose-built devices eliminate interoperability issues that could open up holes
• Integrating hardware, operating system and applications	Yes		Reduce vulnerabilities associated with general purpose operating systems or hardware platforms
• Designed specifically for security	Yes		Simplify the application of patches to quickly address vulnerabilities-only have to apply one, don't need to worry about whether multiple patches will introduce inconsistencies or vulnerabilities
Offers same user interface across product line	Yes		
Quickly accommodates new security functionality to address new security threats	Yes		purpose-built device
Solution dependent on other vendors	No		
Predictable Performance			
Ability to process traffic of varying packet sizes to meet the performance requirements of the network	Yes		See Appendix A for accompanying chart on specific performance numbers for each product
Multiple performance metrics published	Yes		FW throughput in varied packet sizes, packets per second, and VPN throughput published on nearly every datasheet.
• Only vendor to publish packets per second	Yes		A true measure of FW performance
• Only vendor to publish IMIX as well as std big packets	Yes		IMIX (Internet mix) is more representative of traffic traversing a customer's network and is made up of 58.33% 64 byte packets + 33.33% 570 byte packets + 8.33% 1518 byte packets of UDP traffic.
• Only vendor to publish 64 byte packets as well as std big packets			64 byte packets are most demanding type of traffic.
Can scale from a small remote user to a large central site to eliminate weak links	Yes		Juniper Networks provides a complete line of platforms for small, home office up to large data center environments. See Appendix A for more information.
Able to deliver consistent performance under load:			
• Purpose-built device that is not constrained by software or	Yes		

hardware designs			
• Not discrete functions - integrates platform, OS and applications with the networking capabilities needed to deliver security	Yes		
• Custom ASIC accelerates intensive processing for key platforms	Yes		
Optimized traffic processing:			
• Purpose-built device – tightly integrates functionality with the ability to share resources and maximize performance	Yes		
• Security Specific Processing - Streamlined, linear packet processing (reduced memory copying and unnecessary traversals of PCI busses)	Yes		
• Each processing component is optimized	Yes		
Traffic prioritization to ensure business critical applications are available	Yes		
Deliver Quality of Service (QoS):	Yes		
• Control bandwidth at Policy level, interface level or both	Yes		
• Set priority field in the Type of Service (TOS) byte to reflect traffic class priority	Ye		
• Support DSCP (DiffServe Stamping)	Yes		
Provide additional new functionality without degrading performance	Yes		
Fast session ramp rates to protect against DoS attacks	Yes		
Dedicated hardware, allowing separate paths for session set up and established flows	Yes		
Predictable Performance - VPN Specific			
Accelerate IKE negotiations for quick tunnel set up OS and Hardware designed specifically to negotiate security associations	Yes		Purpose built solutions can develop process efficiencies over general purpose OS
Minimal latency to ensure real-time applications are not degraded:	Yes		
Provides fast path for established flows	Yes		
Packets are quickly processed without unnecessary traversals of PCI busses	Yes		Unnecessary traversals of PCI busses is a common problem with PC-based platforms using VPN acceleration cards, adding latency to application.
Maintain large numbers of tunnels to ensure availability	Yes		
Branch Device Consolidation			
Proven security platform	Yes		
Integrates best-in-class UTM	Yes		

technologies			
Added HW is not required to run UTM	Yes		
Routing engine proven to address traditional branch office requirements	Yes		
Supports integrated WAN interfaces	Yes		Wide range of WAN interfaces integrated into the SSG Family to facilitate elimination of external connectivity devices.
• ADSL/ADSL 2+	Yes		
• T1/E1	Yes		
• DS3	Yes		
• ISDN	Yes		
• V.92	Yes		
• Serial	Yes		
Supports WAN encapsulations (HDLC, PPP, MLPPP, FR, MLFR)	Yes		
Supports LAN routing protocols (OSPF, BGP, RIP v1/2)	Yes		
Modular form factor to eliminate truck roll upgrades	Yes		
Fault Tolerance – High Availability, Resiliency			
Device, itself, provides redundancy:	Yes		
Solid-state Redundant components (fans/power supplies)	Yes		
Port Density	Yes		
Supports dynamic routing protocols:	Yes		Enables the survival of failures at the transport level –needed for other components of resiliency
OSPF	Yes		
BGP	Yes		
RIPv1/2	Yes		
High Availability (HA)	Yes		
Configurations to reduce single point of failure	Yes		
Stateful (sharing session information) to maintain connections	Yes		
Active-passive HA (one device processing traffic, with the second device as a back-up)	Yes		
Active-active HA (both devices processing traffic)	Yes		
Active-active, full-mesh HA to survive a failure up or downstream from device	Yes		
Redundant physical connections (e.g. connections to different service providers)	Yes		Note: need to support dynamic routing to do this
Dial back-up	Yes		
Alternate transport options:			
• ADSL/ADSL 2+	Yes		
• T1/E1	Yes		
• DS3	Yes		
• ISDN	Yes		
• V.92	Yes		
• Serial	Yes		

A high Mean Time Before Failure (MTBF) expectancy	Yes		Using Bellcore MTBF calculations
Fault Tolerance - VPN Specific			
Ability to run dynamic routing through its tunnels to automatically learn the network and route around failures	Yes		Juniper Networks Dynamic Route-based VPNs
Product's HA performs VPN synch (sharing VPN state information) to maintain the VPN connection in the event of a failure	Yes		Note: most routers cannot offer this functionality
Supports multiple tunnels, running the same services, between VPN gateways	Yes		Note: Rule-based or Policy-based VPNs cannot do this, only route-based and dynamic route-based VPNs
Supports fail-over between tunnels based on alternate static routes defined in the route table	Yes		For route-based VPNs, can take up to a minute for fail-over
Supports fail-over between redundant tunnels using dynamic routing	Yes		For dynamic route-based VPNs, can take up to a minute for fail-over
Supports fail-over between redundant tunnels using another mechanism	Yes		VPN Path Monitor, in conjunction with dynamic route-based VPNs support configurable interval to allow sub-second fail-over
R-associate VPN with another tunnel without having to renegotiate the encryption keys	Yes		Uses Security Association mirroring mechanism
Ease of Use			
Multiple management mechanisms for flexibility			
• CLI	Yes		
• WebUI	Yes		
• Centralized Management	Yes		
On-line help	Yes		
Broad array of support options	Yes		http://www.Juniper.Net/support
Support is delivered by a single vendor with a single support contract	Yes		
Remote management options:			
• SSH	Yes		
• Telnet	Yes		
• Web (HTTP/HTTPs)	Yes		
• Centralized Management GUI	Yes		
• Syslog	Yes		
• SNMP	Yes		
• Ping for remote monitoring	Yes		
Policy changes can be distributed quickly to one or many devices	Yes		via NSM
Management of firewall and VPN functionality from a single console	Yes		
View Firewall and VPN logs and status from a single console	Yes		
Firewall policies can be easily applied to VPN traffic, without having to define the network (I-based) within that policy	Yes		Security Zones, Virtual LANs and virtual routers
Policies can be easily applied to new networks	Yes		Security Zones, Virtual LANs and virtual routers

Different network segments can have different policy sets, effectively segmenting the network	Yes		Security Zones, Virtual LANs and virtual routers
Administrators can apply universal rules to multiple security zones	Yes		
Different network segments, departments, offices, etc. can manage their own security, completely separate from each other:	Yes		Juniper Networks Virtual Systems
• Separate management of devices	Yes		
• Separate "view"	Yes		
Built in troubleshooting features:	Yes		
• Contextual information in logs	Yes		
• Identification of failures in logs	Yes		
• Web-based trouble shooting	Yes		
Ability to integrate with other management and enterprise platforms/systems:			
• SNMP traps	Yes		
• MIP	Yes		
• MIB	Yes		
• CLI via SSH for configuration	Yes		
• Syslog	Yes		
• NTP	Yes		Note: NTP integration allows internal clocks to be synchronized to ensure log files have accurate time stamps
Ease of Use - VPN Specific			
New networks can be easily added to the VPN utilizing dynamic routing	Yes		
Reroute around problems with minimal human intervention	Yes		
Dynamic routing automatically finds available routes	Yes		
Route-based VPNs can switch to alternate routes in route table	Yes		
Flexibility to do complex VPN configurations (e.g. hybrid full mesh, hub and spoke)	Yes		
Rule-based VPNs	Yes		
Route-based Dynamic Route-Based	Yes		
Simple Deployment and Installation			
Delivered as an appliance for simple deployment	Yes		
Delivered as software that has to be loaded onto hardware	No		Can introduce interoperability issues
Multiple deployment options:	Yes		
• Transparent mode	Yes		
• Route mode	Yes		
• NAT	Yes		
Multiple management mechanisms for flexibility			
• CLI	Yes		
• WebUI	Yes		
• Centralized Management	Yes		
Wizards to guide an administrator	Yes		

through tasks such as initial configuration, policy install, VPN set up			
Single patches that apply to the platform, OS and applications	Yes		Not possible if applications, OS and hardware are not fully integrated or from the same vendor
Integrated key networking functionality for easy integration into a network environment			
• Dynamic routing protocols	Yes		
• Virtual Routers	Yes		
• Support multiple routing domains	Yes		
• Multiple methods of address translation	Yes		
• Dynamic IPs (DIPs)	Yes		Support of DIPs allows policy-based address translations using pools of IP addresses to handle overlapping IP addresses.
• Support Mapped IPs (MIPs)	Yes		MIPs provide one-to-one IP mapping for internal servers
• Support Virtual IPs (VIPs)	Yes		VIPs provides mapping of protocols from one public external IP to multiple internal private IPs based on the port. Allows one IP address to support Web, FTP, e-mail and other servers.
• Supports Policy-based NAT/PAT	Yes		
Tools and services to facilitate migration from other Firewall/VPN products	Yes		
Features for Remote Users and Offices			
Remote User solution including VPN and personal firewall	Yes		
Remote office appliance for easy installation	Yes		purpose-built device
Firewall and VPN solutions are integrated to ensure no compromises in security occur at remote site	Yes		Eliminates “weak” links with affordable solutions
Provides strong remote site security:			
• Integrated functionality to ensure consistent security,	Yes		
• Split tunneling support	Yes		
• Separate home and work zones	Yes		
Supports a dial-back-up option to ensure connectivity at a remote office	Yes		
Easy to manage to ensure security experts don’t need to be on site	Yes		
Managed using the same console as large central site solutions to ensure consistent policy enforcement is consistent	Yes		
Can be managed centrally	Yes		

Appendix A: Juniper Networks Integrated FW/IPSec VPN Product Specifications

Juniper Networks Firewall/VPN Products	Interfaces	Max Throughput	Max Sessions	Max VPN Tunnels	Max Policies	Virtual Systems	Virtual LANs	Security Zones	Virtual Routers	High Availability[1]	Routing	Deep Inspection / IDP	Integrated Antivirus[5]	Integrated Anti-Spam	Web Filtering (Integrated/External)
NetScreen-5400[4]	6 XFP 10Gig (SR or LR) OR 24 Mini-GBIC	30 Gb FW 15 Gb AES VPN	1,000,000	25,000	40,000	Up to 500	4,000	16 + up to 1,000 addtl[2]	3 + up to 500 addtl[2]	A/P, A/A, F/M	OSPF, BGP, RIPv1/v2	Yes / No	No	No	No / Yes
NetScreen-5200[4]	2 XFP 10Gig (SR or LR) OR 8 Mini-GBIC	10 Gb FW 5 Gb AES VPN	1,000,000	25,000	40,000	Up to 500	4,000	16 + up to 1,000 addtl[2]	3 + up to 500 addtl[2]	A/P, A/A, F/M	OSPF, BGP, RIPv1/v2	Yes / No	No	No	No / Yes
ISG 2000 w/optional IDP	Up to 8 Mini-GBIC (SX or LX), or up to 8 10/100/1000, or up to 28 10/100	4 Gb FW 2 Gb 3DES VPN	1,000,000[6]	10,000	30,000	Up to 50	2,000[6]	26 + up to 100 addtl[2]	3 + up to 50 addtl[2]	A/P, A/A, F/M	OSPF, BGP, RIPv1/v2	Yes / Yes	No	Yes	Yes / Yes
ISG 1000 w/optional IDP	4 fixed CG plus up to 4 Mini-GBIC (SX or LX), or up to 8 10/100/1000, or 20 10/100	1 Gb FW 1 Gb 3DES VPN	500,000[6]	2,000	10,000	Up to 10	1,000[6]	20 + up to 20 addtl[2]	3 + up to 10 addtl[2]	A/P, A/A, F/M	OSPF, BGP, RIPv1/v2	Yes / Yes	No	Yes	Yes / Yes
NetScreen-500[4]	Up to 8 10/100 OR 8 Mini-GBIC OR 4 GBIC	700 Mb FW 250 Mb 3DES VPN	250,000	5,000 + 10,000 Dial-up	20,000	Up to 25	100	8 + up to 50 addtl[2]	3 + up to 25 addtl[2]	A/P, A/A, F/M	OSPF, BGP, RIPv1/v2	Yes / No	No	No	No / Yes
SSG 550 **SSG 550M**	4 fixed CG + 6 I/O slots supporting 1xSFP, 1xCG, 4xFE, 2xSerial, 2xT1/E1, 1xDS3	1+ Gb FW 500 Mb 3DES VPN 600,000 Packets per second	128,000	1,000	4,000	N/A	150	60	8	A/A, A/P	OSPF, BGP, RIPv1/v2, Frame Relay, Multilink Frame Relay, PPP, Multilink PPP, HDLC	Yes / No	Yes	Yes	Yes / Yes
SSG 520 **SSG 520M**	4 fixed CG + 6 I/O slots supporting 1xSFP, 1xCG, 4xFE, 2xSerial, 2xT1/E1, 1xDS3	650+ Mb FW 300 Mb 3DES VPN 300,000 Packets per second	64,000	500	1,000	N/A	125	60	5	A/P	OSPF, BGP, RIPv1/v2, Frame Relay, Multilink Frame Relay, PPP, Multilink PPP, HDLC	Yes / No	Yes	Yes	Yes / Yes
NetScreen-204/208[4]	4 10/100 (NS204) 8 10/100 (NS208)	375 Mb FW 175 Mb 3DES VPN	128,000	1,000	4,000	N/A	32 + up to 96 addtl[3]	4 + up to 10 addtl[3] (NS204) 8 + up to 10 addtl[3] (NS208)	3 + up to 5 addtl[3]	A/P, A/A (NS204) A/P, A/A, F/M (NS208)	OSPF, BGP, RIPv1/v2	Yes / No	No	No	No / Yes
NetScreen-50	4 10/100	170 Mb FW 45 Mb 3DES VPN	64,000	500	1,000	N/A	16	4	3	A/P	OSPF, BGP, RIPv1/v2	Yes / No	No	Yes	Yes / Yes
SSG 140	8 10/100 + 2 10/100/1000 + 4 I/O slots supporting T1, E1, ISDN BRI S/T, Serial	350+ Mb FW 100 Mb 3DES VPN	32,000	125	500	N/A	100	40	3	A/P	OSPF, BGP, RIPv1/v2, Frame Relay, Multilink Frame Relay, PPP, Multilink PPP, HDLC	Yes / No	Yes	Yes	Yes / Yes
NetScreen-25	4 10/100	100 Mb FW 20 Mb 3DES VPN	32,000	125	500	N/A	16	4	3	H/A Lite	OSPF, BGP, RIPv1/v2	Yes / No	No	Yes	Yes / Yes
SSG 20 **SSG 20 Wireless**	5 10/100 + 2 I/O slots supporting T1, E1, V.92, ISDN BRI S/T, or ADSL2+. Optional 802.11a/b/g	160 Mb FW 40 Mb 3DES VPN	4,000/ 8,000[7]	25/40[7]	200	N/A	10/50[7]	8	3	Dial Backup, A/P[7]	OSPF, BGP, RIPv1/v2, Frame Relay, Multilink Frame Relay, PPP, Multilink PPP, HDLC	Yes / No	Yes	Yes	Yes / Yes
SSG 5 **SSG 5 Wireless**	7 10/100 with Factory Configured V.92 or ISDN BRI S/T or RS232 Serial/Aux. Optional 802.11a/b/g	160 Mb FW 40 Mb 3DES VPN	4,000/ 8,000[7]	25/40[7]	200	N/A	10/50[7]	8	3	Dial Backup, A/P[7]	OSPF, BGP, RIPv1/v2, PPP	Yes / No	Yes	Yes	Yes / Yes
NetScreen-5GT **NetScreen-5GT ADSL** **NetScreen-5GT Wireless**	5 10/100 + Factory Configured ADSL and/or 802.11b/g	75 Mb FW 20 Mb 3DES VPN	2,000	10	100	N/A	N/A	2 (3 with home /work zones) 4 (NS 5GT Wireless)	3	Dial Backup	OSPF, BGP, RIPv1/v2	Yes / No	Yes	Yes	Yes / Yes
NetScreen-5XT[4]	5 10/100	70 Mb FW 20 Mb 3DES VPN	2,000	10	100	N/A	N/A	2 (3 with home /work zones)	2	Dial Backup	OSPF, BGP, RIPv1/v2	Yes / No	No	No	No / Yes
NetScreen-Hardware Security Client	5 10/100	50 Mb FW 10 Mb 3DES VPN	1,000	2	50	N/A	N/A	2 (3 with home /work zones)	2	No	RIPv1/v2	Yes / No	Yes	Yes	Yes / Yes

1) High Availability definitions: A/P = Active / Passive mode, A/A = Active / Active mode, F/M = Active / Active full mesh mode, H/A Lite = FW and VPN failover without session synchronization
2) Requires purchase of virtual system key; Every virtual system includes one virtual router and two security zones, usable in the virtual or root system
3) 96 VLANs, 10 security zones and 5 virtual routers can be added to the NetScreen-200 series with the purchase of a virtualization key
4) Please visit http://csrc.nist.gov/cryptval/140-1/1401vend.htm for FIPS 140-2 certificates for these platforms.
5) The Juniper-Kaspersky Antivirus engine includes protection against Spyware, Adware, and Phishing attacks.
6) Max Sessions listed based on optional IDP upgrade. FW/VPN Max Sessions without optional IDP upgrade are 250,000 for the ISG 1000 and 500,000 for the ISG 2000. VLAN Maximums are 250 for the ISG 1000 and 500 for the ISG 2000
7) Increased Session, VPN tunnel, VLAN capacities, A/P HA and HA Lite require an Extended License key.

For the most updated product specifications table, please visit http://www.juniper.net/products/glance/all_nscn_products.pdf