

Buyer's Guide For Integrated Firewall and Virtual Private Network Solutions



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

Part Number: 710008-001 June 2004

Table of Contents

Introduction.....	3
Executive Summary.....	4
Quick Checklist.....	6
Detailed Buyer’s Checklist.....	8
1. Strong Security.....	8
2. Predictable Performance.....	12
3. Fault Tolerant – High Availability, Resiliency.....	13
4. Ease of Use.....	15
5. Simple Deployment and Installation.....	17
Features for Remote Users and Offices.....	18
Features for Wireless.....	18

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 step that organizations generally take is to control who and what gets in and out of the network by deploying a firewall. Firewalls perform access control, user authentication, traffic management and policy enforcement to ensure only appropriate users and services are able to traverse the network and that business applications are given priority. Firewalls, however, 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 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, attackers are increasingly attacking vulnerabilities found not at the network-level, but at the application-layer, and are actually leveraging traffic "allowed" by the firewall to get into the network. As a result, some firewalls have started to look deeper into the traffic they are allowing in and out of the network to try to identify and prevent attacks found at the application-layer.

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

Firewall/IPSec VPNs serve as the foundation upon which a strong security stance can be built, so the purchase decision should be framed in terms that support a long-term investment that can be leveraged as the organization's needs 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 put a strain on 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 solution choice.

1. 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 included is strong access control, user authentication, attack protection - both at the network and application-layer - IPSec and encryption choices for data integrity, and network segmentation for attack containment. 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. It is especially important, however, to scrutinize the feature set of products that integrate multiple functions to ensure they are not too simplistic in their approach and are not lacking all of the robust, proven features that are required for strong security. While initially appealing because they seem to be easy to manage, an integrated solution that does not marry best-of-breed functionality can actually end up creating more work due to the security holes they allow. For example, how effective is it to have intrusion prevention integration that can only stop network-layer attacks? In response, it is more important that the solution provides the granularity and flexibility needed to identify differences in traffic and appropriately process that traffic than to satisfy a checklist. 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. The solution should be designed for and deliver security to justify its deployment.

2. Offer predictable performance.

The solution 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 segment that 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.

3. Deliver a high level of fault tolerance to ensure the solution is always available.

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 VPN state information and survive a failure both up and down stream of the device, offering 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.

4. 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. An administrator should be able to manage the device, network and security aspects of the solution, from a single interface, as opposed to having to go to one interface to make routing changes and another interface to set security policies. It should automate as much as possible to minimize human intervention, using tools such as templates and auto-configurations to maximize consistent security deployments throughout the network. It should also, however, provide granular controls to ensure that specific sites have a configuration that is most appropriate to their environment. It should enable different people in the organization to efficiently do their jobs, without introducing any risk to the security at large. For example, a NOC administrator should be able to get access to device status, but shouldn't be able to make security policy changes, a CIO should be able to see reports, but not make routing changes, etc. It should also be easy to troubleshoot to enable organizations to quickly resolve problems. 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.

5. 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. It 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.

Quick Checklist

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.

1. Provide Strong Security

- Does the solution integrate best-of-breed technologies?
 - How long have the technologies been in the market?
 - Are there any third party verifications of viability available?
 - Are the technologies based on open source solutions?
- Does the solution provide strong access control – stateful inspection?
- What kind of user authentication does the solution support?
- What network-level attacks does the solution protect against?
 - DoS attacks
 - DDoS attacks
- Does it have the ability to make determinations on whether to allow or deny traffic based on application-layer information?
 - What kind of application-level attacks can it detect?
 - What kind of application-level attacks can it prevent?
- What kind of encryption does the VPN support?
- Can the solution apply policies to internal traffic to establish additional layers of trust and contain attacks?
- What type of security certifications does the product have?
- What kind of platform is the solution built on?
 - Is it a general-purpose platform that could introduce security risks?
- Can the solution scale to meet the different security needs of small to large sites?

2. Offer Predictable Performance

- What are the performance (large and small packet size) capabilities of the solution to ensure that performance remains predictable?
- What has the solution done to optimize its traffic processing?
- How does the solution minimize latency to ensure real-time applications are not degraded (e.g. VoIP)?
- How does the solution handle very fast session ramp rates to protect against DoS attacks?
- How does the architecture of the solution enable performance under load?
- How does the solution handle multiple concurrent sessions to ensure user connectivity is not lost or slowed?
- How does the solution accommodate additional functionality, without degrading performance?
- How does the solution accelerate the VPN negotiation to set up the VPN tunnels to make the time imperceptible to the user?
- How can the solution quickly create and then maintain VPN tunnels to ensure they are always available for the user?

3. Deliver a high level of fault tolerance to ensure the solution is always available

- Does the solution support high availability (HA) configurations, including active/active, full mesh, to reduce the chance of a single point of failure?
- 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?
- Can the solution take advantage of dynamic routing as part of VPN resiliency?
- Can the solution support redundant paths? If so, what kind – multiple ISPs, dial back-up?
- What redundancy features have been built into the VPN configuration?
- What are the mechanisms used to minimize fail-over latency and ensure maximum uptime?

4. Offer ease of use and management.

- Are there multiple ways to interact and manage the system?
- How easy is it to perform management tasks?
 - Can device, network and security configurations be managed using the same interface?
- Does the system grant different people in the organization different access privileges?
 - How does the system ensure that people are only accessing what they need to access?
 - How easy is it to set up or change a role to ensure access privileges map to current employee activity?
- How quickly can changes be made in a large distributed network?
- Are there configuration templates to simplify deployments?
 - How easy is it to customize the template information for specific site deployments?
- How easy is it to troubleshoot problems?
 - Is there a way to roll back to a previous configuration if changes affect the connectivity of the solution?
- How much manual intervention is needed when a VPN connection goes down?
- Can firewall policies be easily applied to VPN traffic, without a lot of additional configuration?
- How easy is it to add a network to the VPN?
- How easy is it to configure complex VPN configurations, such as a hybrid full-mesh and hub and spoke?

5. Enable quick and simple deployment and installation

- Are there different options that accommodate administrator preferences for installing and configuring the system?
- What kind of platform is the solution running on?
 - Is the solution based on a general-purpose platform?
 - Is the solution delivered as an appliance for easy deployment?
- How easy is it to deploy a device in the field?
 - What level of technical expertise is required?
 - Can it be managed centrally?
- Does the solution have a transparent deployment mode that does not require routing changes to the network?
- What routing protocols does the solution support?
- What networking features does the solution support to facilitate a timely deployment?
- How are patches applied?

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 / IPSec VPN / Deep Inspection Solutions*	Alternate Solution:	Notes
1. Strong Security			
Performs Stateful Inspection	Yes		
Protects against network-level attacks	Yes		e.g. IP fragmentation, ICMP "ping of death"
Protects against DoS and DDoS attacks	Yes		e.g. Syn, UDP, ICMP Floods
Protects against transport layer attacks	Yes		e.g. Port scans, Tear Drop attack
Protects against application-layer attacks: e-mail Web FTP DNS	Yes Yes (SMTP, POP, IMAP) Yes Yes		e.g. Nimda Worm, Code Red Worm
Uses proxies for attack detection	No		The use of proxies can result in significant performance degradation
Uses Stateful signatures for attack detection	Yes		
Uses protocol enforcement for attack detection	Yes		
Blocks malicious URLs	Yes, matches user defined patterns		
Protects against viruses	Yes, low-end products have embedded antivirus		
Options for strong user authentication: <i>Web Auth</i> <i>Tokens</i> User name/Password: <i>HTTP</i> <i>FTP</i> <i>Telnet</i>	Yes Yes Yes Yes Yes		
Options for strong user verification: <i>RADIUS</i> <i>Internal Database</i> <i>LDAP</i> <i>SecureID</i>	Yes Yes Yes Yes		
Built in attack containment			

capabilities <ul style="list-style-type: none"> Ability to apply policies to restrict traffic between internal network segments 	Yes, Security Zones		
Ability to split network into <u>completely separate domains</u> and create security policies for each one <ul style="list-style-type: none"> Completely separate policies Completely separate administrative controls 	Yes, Virtual Systems Yes Yes		
Certifications: <ul style="list-style-type: none"> Common Criteria ICSA certification 	Yes Yes		
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
Strong encryption options: <i>AES</i> <i>DES</i> <i>3DES</i>	Yes Yes Yes		
Options for strong user authentication: <i>Xauth</i> <i>Web Auth</i> <i>X.509 certificates</i> <i>Tokens</i> <i>User name/Password</i>	Yes Yes Yes Yes Yes		
Options for strong user verification: <i>RADIUS</i> <i>Internal Database</i> <i>LDAP</i> <i>SecureID</i> <i>X.509 certificates</i>	Yes Yes Yes Yes Yes		
Certifications: <ul style="list-style-type: none"> FIPS 140-1 or 140-2 ICSA IPSec 	Yes Yes		
Integration/System Design			
The number of applications delivered in the solution	FW/VPN/Deep Inspection -- Antivirus also included in low-end		
The source of the applications are:			
Proprietary	Yes – FW/VPN/Deep Inspection		
Partnerships	Yes, antivirus through Trend Micro partnership		
OEM relationships	Yes, Remote client via		

Open source code	Safenet No		
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	FW/VPN/Deep Inspection (Gartner Magic Quadrant)		
All functionality managed with the same console	FW/VPN/Deep Inspection managed with same interface/console		Simplifies deployment, reduces chance for human error that could result in vulnerabilities
<p>Built in features that protect against tampering:</p> <ul style="list-style-type: none"> • Packaging sealed with custom tape • Uses tamper seals to indicate authenticity • Hardware can restrict remote access via access lists • Access list creation based on IP and MAC addresses • Hardware protects against password overrides • Hardware uses secure connections for remote access • Custom OS built for security • OS is hardened • FIPs certified for physical protection of keys and configuration, as well as software protection 	<p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p>		<ul style="list-style-type: none"> • A custom OS is less prone to known attacks than a general purpose OS
<p>Guards against vulnerabilities within the system itself:</p> <ul style="list-style-type: none"> • The number of different patches that need to potentially be applied • The general purpose systems or platforms that are used 	<p>One, Juniper Networks uses a single OS</p> <p>None, purpose-built appliance with custom OS</p>		
	<ul style="list-style-type: none"> • Juniper Networks NetScreen-Remote or Juniper Networks NetScreen-Secure Access (SSL) for remote/mobile users 		

<p>Can scale from a small remote user to a large central site to eliminate weak links</p>	<ul style="list-style-type: none"> • Juniper Networks NetScreen-5XT, 5GT series for remote/home offices • Juniper Networks NetScreen-25 & -50 for branch office or small central site • Juniper Networks NetScreen-200 series for medium central site, regional offices • Juniper Networks NetScreen-500 and Juniper Networks NetScreen-ISG 2000 for large central sites • Juniper Networks NetScreen-5000 series for large central sites, data centers, service providers 		
<p>Solution dependent on other vendors to make changes or innovations</p>	<p>No</p>		
<p>Applications under load continue to perform all security functionality</p>	<p>No</p>		<p>Some solutions simply pass traffic when under load – creating security risk</p>

2. Predictable Performance			
Ability to process traffic of varying packet sizes to meet the performance requirements of the network	Yes, See Tolly Reports for third party verification		
Accelerates intensive processing with hardware	Yes, including custom security ASICs		
Ability to support applications with a low tolerance for latency/jitter, such as VoIP, multimedia, etc.	Yes, hardware is optimized for streamlined processing		
Fast session ramp rates to protect against DoS attacks	Yes, Dedicated hardware, allowing separate paths for session set up and established flows		
Provide additional functionality without degrading performance	Yes, <ul style="list-style-type: none"> • ASIC/FPGAs offload intensive processing, making CPU available for new/additional functions • Programmability in ASIC to accelerate future functions 		
Turning on all applications does not affect the solutions ability to meet the performance needs of the deployment	See spec sheets for performance numbers		
Traffic prioritization to ensure business critical applications are available	Yes		
Deliver Quality of Service (QoS): <ul style="list-style-type: none"> o Control bandwidth o Set priority field in the Type of Service (TOS) byte to reflect traffic class priority 	Yes Yes		
VPN Specific			
Accelerate IKE negotiations for quick tunnel set up	Yes, OS and Hardware designed specifically to negotiate security associations		Purpose built solutions can develop process efficiencies over general purpose OS'
Minimal latency to ensure real-time applications are not degraded:	Yes, <ul style="list-style-type: none"> o Provides fast path for established flows o Packets are quickly processed without unnecessary traversals of PCI busses 		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		

3. Fault Tolerant – High Availability, Resiliency			
Device, itself, provides redundancy: <ul style="list-style-type: none"> ○ Solid-state ○ Redundant components (fans/power supplies) ○ Port Density 	Yes Yes Yes		
Supports dynamic routing protocols: <ul style="list-style-type: none"> ○ OSPF ○ BGP ○ RIP 	Yes Yes Yes		Enables the survival of failures at the transport level –needed for other components of resiliency
High Availability (HA) Configurations to reduce single point of failure: <ul style="list-style-type: none"> ○ Stateful (sharing session information) to maintain connections ○ VPN sync (sharing VPN information to maintain security association in the event of a failure) ○ Active-passive HA (one device processing traffic, with the second device as a back-up) ○ Active-active HA (both devices processing traffic) ○ Active-active, full-mesh HA to survive a failure up or downstream from device 	Yes Yes Yes Yes Yes		
Redundant physical connections (e.g. connections to different service providers)	Yes		Note: need to support dynamic routing to do this
Alternate transport options, such as: <ul style="list-style-type: none"> ○ DSL ○ Dial back-up 	Yes Yes		
A high Mean Time Before Failure (MTBF) expectancy	Yes, using Bellcore MTBF calculations		
VPN Specific			
Ability to run dynamic routing through its tunnels to automatically learn the network and route around failures	Yes, Dynamic Route-based VPNs (Best Path VPNs)		
Product's HA performs VPN sync (sharing VPN state information) to maintain the VPN connection in the event of a failure	Yes		Note: most routers cannot offer this functionality

Supports different VPN deployment modes: Rule-based/Policy-based Route-based Dynamic Route-based (Best Path)	Yes Yes Yes		
Support multiple VPN gateways to enable VPN to persist in the event of a failure	Yes		For rule-based or policy-based VPNs
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, custom VPN Path Monitor-configurable interval to allow fail-over in seconds		
R-associate VPN with another tunnel without having to renegotiate the encryption keys	Yes, Security Association mirroring mechanism		

4. Ease of Use			
Multiple ways to interact with the system: <ul style="list-style-type: none"> o CLI o Web UI o Central Management Platform 	<p>Yes</p> <p>Yes</p> <p>Yes</p>		
Remote management options: <ul style="list-style-type: none"> o SSH o Telnet o Web (HTTP/HTTPS) o Centralized Management GUI o Syslog o SNMP o Ping for remote monitoring 	<p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p>		
Ability to manage the device, network and security functionality from a single console	Yes, Juniper Networks NetScreen-Security Manager		
Ability to view all logs in central location	Yes		
Ability to assign different people in the organization different read/write privileges	Yes, role-based administration		
Policy changes can be distributed quickly to one or many devices	Yes, Juniper Networks NetScreen-Security Manager		
Firewall policies can be easily applied to VPN traffic, without having to define the network (IP-based) within that policy	Yes, using Security Zones		See Juniper Networks VPN White Paper "Dynamic VPNs Achieving Scalable, Secure Site-to-Site Connectivity"
Policies can be easily applied to new networks/interfaces	Yes, using Security Zones		
Offers VLAN support to integrate subnets easily	Yes		
Different network segments can have different policy sets, effectively segmenting the network	Yes, using Security Zones		
Administrators can apply universal rules to multiple security zones	Yes, unique to NetScreen		
Different network segments, departments, offices, etc. can manage their own security, completely separate from each other: <ul style="list-style-type: none"> o Separate management devices o Separate "view" 	<p>Yes</p> <p>Yes</p>		
Built in troubleshooting features: <ul style="list-style-type: none"> o Contextual information 	Yes		

<ul style="list-style-type: none"> o in logs o Identification of failures in logs o Web-based trouble shooting 	<p>Yes</p> <p>Yes</p>		
Offers roll-back option to last-known "good" configuration, if changes do not "work"	Yes		
Ability to integrate with other management and enterprise platforms/systems: <ul style="list-style-type: none"> o SNMP traps o MIP o MIB o CLI via SSH for configuration o Syslog o NTP 	<p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p>		Note: NTP integration allows internal clocks to be synchronized to ensure log files have accurate time stamps
On-line help	Yes		
Broad array of support options	Yes		
Support is delivered by a single vendor with a single support contract	Yes		
VPN Specific			
New networks can be easily added to the VPN	Yes, utilizing dynamic routing and Security Zones		
Reroute around problems with minimal human intervention	Yes, <ul style="list-style-type: none"> o Dynamic routing automatically finds available routes o Route-based VPNs can switch to alternate routes in route table 		
Flexibility to do complex VPN configurations (e.g. hybrid full mesh, hub and spoke) using: <ul style="list-style-type: none"> o Rule-based VPNs o Route-based o Dynamic Route-Based 	<p>Yes</p> <p>Yes</p> <p>Yes</p>		

5. 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: <ul style="list-style-type: none"> o Transparent mode o Route mode <ul style="list-style-type: none"> o BGP o OSPF o NAT 	Yes Yes Yes Yes Yes, can be done on per policy basis		
Offers multiple ways to interact with the system: <ul style="list-style-type: none"> o Command Line Interface (CLI) o Web interface o Graphical User Interface (GUI)/central management platform 	Yes Yes Yes, Juniper Networks NetScreen-Security Manager		
Wizards to guide an administrator through tasks, such as initial configuration, policy install, VPN set up	Yes		
Templates available for consistent configuration of multiple devices	Yes		
Integrated key networking functionality for easy integration into a network environment, such as: <ul style="list-style-type: none"> o Dynamic routing protocols o Virtual Routers <ul style="list-style-type: none"> o Support multiple routing domains o Multiple methods of address translation <ul style="list-style-type: none"> o Dynamic IPs (DIPs) o Support Mapped IPvLANs (MIPs) o Support Virtual IPs (VIPs) o Supports NAT <ul style="list-style-type: none"> o Policy-based o PAT/NAT capabilities 	Yes Yes Yes Yes Yes Yes Yes Yes Yes		<ul style="list-style-type: none"> o Support of DIPs allows policy-based address translations using pools of IP addresses to handle overlapping IP addresses. o MIPs provide one-to-one IP mapping for internal servers o 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.
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
Ability to maintain the VPN abstraction and continue to leverage dynamic routing when applying the firewall policy	Yes, through Security Zones		If the firewall policy requires the use of IP addresses then the management advantages of dynamic routing are lost.
Tools and services to facilitate migration from other Firewall/VPN products	Yes		

Features for Remote Users and Offices			
Remote User solution including VPN, firewall, virus and application-level protection	Yes		
Provides strong remote site security: <ul style="list-style-type: none"> o Integrated functionality to apply access control to remote traffic o Ability to protect against viruses and application-level attacks o Split tunneling support o Separation of corporate and personal traffic to ensure personal/Internet traffic cannot enter the corporate network through the VPN 	Yes Yes Yes Yes		Eliminates “weak” links with affordable solutions
Supports a dial-back-up option to ensure connectivity at a remote office	Yes		
Remote office appliance for easy installation	Yes, purpose-built device		
Ability to configure a device at the corporate office, so that technical resources are not needed at a remote site	Yes, Rapid Deployment		
Easy to manage to ensure security experts don't need to be on site: <ul style="list-style-type: none"> o Managed using the same console as large central site solutions to ensure consistent policy enforcement is consistent o Can be managed centrally 	Yes Yes		
Features for Wireless			
Can separate wireless traffic and apply a security policy to it to control access	Yes, Security Zones		See Securing Wireless LANS white paper at http://www.netscreen.com/resources/whitepapers/enterprise/

*Please see specific product data sheets for individual product features, available on the Web site at www.juniper.net