

Juniper Networks Secure Services Gateway 520

Product Profile:

Vendor:

Juniper Networks

Product::

Secure Services
Gateway (SSG) 520

Target Markets:

Secure Remote Branch
Enterprise Regional HQ

Testing Period:

February 2006

Report Released:

March 24, 2006

Software Tested:

5.1.0r4.6_ssg

Features Tested:

- Routing Functionality
- Firewall Performance
- NAT Performance
- Deep Inspection Performance
- Site-to-Site VPN Performance
- Multi-function scalability. Simultaneous performance of:
 - Firewall,
 - Site-to-Site VPN
 - NAT
 - Deep Inspection

Executive Summary

Juniper Networks engaged Current Analysis and Iometrix to assess and validate the performance of its new branch office security and routing platform, the Juniper Networks Secure Services Gateway (SSG) 520. Juniper Networks positions the SSG 520 to serve as either a branch office security or unified branch office security and routing platform. Current Analysis and Iometrix crafted a test plan that focused on benchmarking the performance of the SSG 520 with stateful, real-world multi-protocol traffic likely to be found in an enterprise branch office environment. A series of 20 benchmarks were performed to characterize the performance of the SSG 520 in increasingly complex configurations representative of real-world deployments, culminating in a multi-function benchmark measuring performance with stateful inspection firewall, site-to-site IPsec VPN, Network Address Translation and Juniper's Deep Inspection content-layer inspection technology. Tests also validated the SSG 520's ability to sustain performance while managing a 10,000 entry routing table consisting of BGP and OSPF routes.

The following key observations can be made regarding the test results:

- The SSG 520 routes in excess of 300,000 PPS (64-byte packet) throughput, with 5,000 BGP and 5,000 OSPF routes, even while adverse route flapping exists.
- The SSG 520 delivers far in excess of 600 Mbps of sustained routing throughput with an IMIX traffic load, even while adverse route flapping conditions exist.
- The SSG 520 delivers more than 300 Mbps of sustained throughput across an IPsec 3DES VPN tunnel for both 1400 byte frames and IMIX traffic payloads.
- The SSG 520 maintains greater than 300 Mbps of sustained throughput across an IPsec 3DES VPN tunnel with firewall, NAT and Critical-level Deep Inspection functionality enabled using an IMIX traffic payload.

Market Overview and Analysis

The branch office plays an increasingly strategic role in today's corporate environments. The demand for a global workforce and market presence, combined with the growing need to source employee talent from multiple, geographically diverse markets is driving enterprises toward a broadly distributed organizational structure with many branch office locations. Likewise, many organizations are extending their corporate perimeters beyond brick-and-mortar walls to include suppliers, contractors and trusted business partners.

Security has always been a top concern for IT architects, yet extending security beyond the corporate perimeter while maintaining performance and manageability in the branch office has traditionally required multiple purpose-built devices, such as firewall, VPN and router. The business impact of malicious threats mandates a robust security solution that can defend against a broad range of threats without compromising performance.

Many factors are driving the demand for increased performance in the branch office. Massive carrier network build-outs combined with advanced networking services such as carrier Ethernet and fiber to the premise are driving last mile WAN performance to new heights, and driving down the total cost per megabit for business class network connections. Inside the enterprise perimeter, organizations have built large, distributed server infrastructures to compensate for poor WAN performance. These distributed data centers present a real security threat, and demand dedicated network resources to ensure security, and increasingly, to ensure regulatory compliance. Finally, WiFi creates its own set of unique challenges including demand for greater internal bandwidth, multi-zone security and segmentation between users and guests.

A common approach to securing these complex networks is to segment traffic and apply routing and firewalling between different resources. To deliver on security expectations and maintain WAN routing performance, a platform capable of LAN-speed security and forwarding performance is required for the branch office. Many competitors have attempted to address the security challenge with purpose built unified threat management appliances, but few of these devices support native concurrent WAN routing. The Juniper Networks SSG 520 marries the performance of a unified threat management (UTM) security solution with the features and interfaces of a WAN router in a package highly suitable for the enterprise branch. As tested, the SSG 520 includes a full suite of network security functions, and additional UTM features are slated for the second half of 2006.

Objectives

Juniper Networks engaged Current Analysis and iometrix to create and execute a benchmark that validates its performance claims on the SSG 520 platform. Testing objectives were broken into two groups: validating datasheet performance, and pushing the envelope of performance and functionality to characterize the SSG 520's performance under strenuous conditions likely to be found in actual enterprise environments. We ran benchmarks using the following conditions to validate the SSG 520's baseline performance:

Performance Criteria	Traffic Type / Actual Test Conditions	Datasheet	Validated?
Firewall Throughput	IMIX, NAT disabled	600 Mbps	Yes
Packets Per Second	64 byte, NAT disabled	300,000 PPS	Yes
VPN	1400 byte, NAT & IPS disabled	300 Mbps	Yes
IPS/Deep Inspection (DI)	HTTP, 64k page views, NAT & VPN disabled, No attack action taken	300 Mbps	Yes

The baseline tests documented above demonstrate that the SSG 520 meets all of its datasheet performance claims with plenty of performance headroom to spare.

To push the SSG 520 to its limits and characterize the SSG 520's performance in an environment and configuration that represents the real-world enterprise branch office, additional and more complex tests were required. Current Analysis and iometrix crafted a set of benchmarks to press the envelope and test the SSG 520 using dynamic, stateful, multi-protocol traffic that closely represents the traffic in a typical branch office environment.

The following chart summarizes the additional tests that were executed to characterize the performance of the SSG 520 in a real-world enterprise branch scenario:

Performance Criteria	Traffic Type / Conditions	Results
Routing Performance	IMIX & 64-byte, with/without flapping	>300,000 PPS and >600 Mbps
Firewall+NAT+DI	IMIX traffic with threats, DI with "close" action	>300 Mbps
Firewall+NAT+DI+VPN	IMIX traffic and threats, DI with "close" action	>300 Mbps
Firewall+NAT+DI+VPN	IMIX traffic with threats, DI with "close" action, ALL HTTP and ALL DI signatures (900+)	225 – 245 Mbps sustained, respectively

These advanced tests demonstrated that the SSG 520 can stand up not only to standard traffic optimized for benchmarking configurations, but indeed maintains very robust throughput even when configured for maximum security and multi-protocol traffic loads.

Test Methodology

Current Analysis and Iometrix developed a test methodology that emulates the actual traffic patterns and protocols found in the enterprise regional and branch office. Leveraging the NetworkTester and N2X testing platforms from Agilent Technologies, Current Analysis and Iometrix defined a benchmark that uses real, stateful TCP/IP traffic to benchmark the Juniper Networks SSG 520. Stateful traffic most accurately represents the environment found on the enterprise WAN and LAN.

Current Analysis and Iometrix insisted that the stateful test traffic used in the benchmark must accurately represent real-world traffic. While many industry standard benchmarks focus on single protocol, single stream, non-stateful packet blasting, we wanted to subject the Juniper SSG 520 to traffic identical to the type that is found in an actual branch office. For purposes of comparing to Juniper's published benchmarks, we agreed to baseline the SSG 520 using stateful traffic with characteristics similar to the 64-byte and 1,400-byte packet benchmarking practices commonly used in the industry. In return, however, we insisted on executing our benchmarks using fully stateful multi-protocol traffic built using the Internet Mix (IMIX) packet distribution standard. (See the technical note at the end of this document for a detailed description of the IMIX standard.)

Current Analysis and Iometrix also insisted that the SSG 520 be configured in a manner representative of a common enterprise branch office, pressing well beyond the least-loaded configuration used in many "performance drag-races." The results of these advanced benchmarks highlight the true strengths of the Juniper SSG 520 platform.

Current Analysis and Iometrix chose the Agilent NetworkTester platform for its ability to generate multiple concurrent streams of stateful, multi-protocol IP traffic. Tests were designed to benchmark the SSG 520 using both industry standard benchmark packet sizes and using a multi-protocol IMIX distribution.

To test VPN functionality, an additional rule was added to the SSG 520 to tunnel all traffic through an IPsec tunnel terminated at a Juniper ISG 1000. The entire suite of tests for deep inspection, NAT, and firewall functionality were run again in this configuration. Additionally, a baseline benchmark consisting of 1,400 byte packet RTP flows was executed to provide a comparative reference to other industry benchmarks.

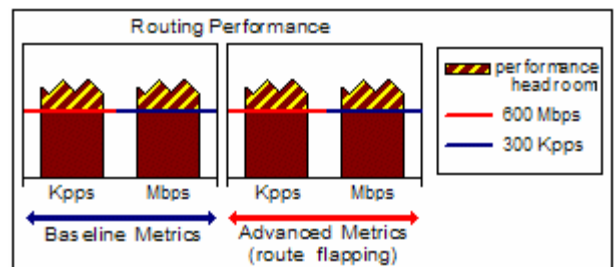
Test Suite 1: Routing Performance and Stability



Test Suite 1 assessed the routing performance and routing robustness of the SSG 520. The Agilent N2X RouterTester was configured to establish 5,000 BGP and 5,000 OSPF route peers with the SSG 520, while Agilent NetworkTesters were configured to send stateful traffic through the SSG 520. After steady state performance was obtained, the N2X additionally introduced periodic route flaps where 1,000 routes were added or removed from service at intervals of ten seconds. In these tests, the SSG 520 was configured with its interfaces in routing mode. A single firewall rule “allow all” was configured between the two routed interfaces (at least one rule must be present on the SSG 520). The test equipment was connected through a LAN switch to Gigabit Ethernet modules installed in the high-speed I/O slots in the SSG 520 chassis. On the NetworkTester platform, test scripts emulating 64-byte telnet traffic and 64-byte RTP traffic were used to measure small packet performance, while scripts consisting of HTTP, Telnet and RTP were used to provide an accurate IMIX load to the SSG 520. All tests were configured to emulate 250 unique users.

Test Suite 1 Results

Test Suite 1 was performed using 64-byte traffic and IMIX traffic profiles. Routing performance was measured in both steady-state operation and during route-flapping events. In small packet tests, the SSG 520 delivered well above its rated 300,000 PPS datasheet performance, even with its route table populated with 10,000 routes. The SSG 520 had sufficient performance headroom to maintain 300,000 PPS (64 byte packets) even when performance dropped due to severe simulated route flapping events. The IMIX throughput tests far exceeded the 600 Mbps datasheet capacity of the SSG 520, and showed no signs of throughput degradation during route flapping events.



These tests demonstrate that the SSG 520 has a stable, reliable, and high performance routing engine that is capable of supporting up to 10,000 network routes, and remains reliable while delivering full throughput even during severe network topology changes.

Test Suite 2: Firewall/IPS/NAT Performance



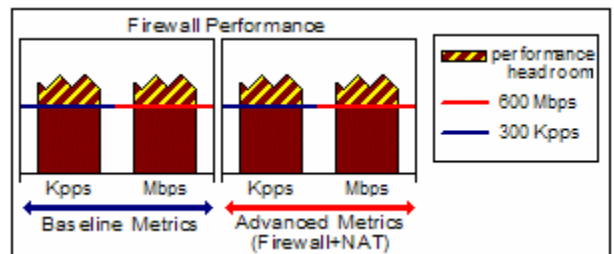
Test Suite 2 assessed the performance of SSG 520 security features. Agilent NetworkTester traffic was aggregated through a LAN switch connected to Gigabit Ethernet modules installed in the high-speed I/O slots of the SSG 520 chassis. The SSG was configured with 100 background firewall rules and 5 explicit deny rules, followed by an explicit “allow all”. This configuration forces the firewall to exercise its policy lookup engine for each flow, and represents a configuration typical of an actual enterprise branch office.

The configuration of the SSG 520 was expanded incrementally to include first standalone firewalling, then NAT+Firewall, then NAT+Firewall+Deep Inspection (IPS). A Deep Inspection performance baseline was established using purely HTTP traffic with HTTP:CRITICAL and HTTP:LOW signatures enabled, both with and without NAT. The HTTP traffic profile consisted of 250 clients requesting a 64K Web page as rapidly as possible.

Additional tests were run using a modified traffic profile consisting of HTTP, FTP, DNS and actual malicious threat traffic, representative of traffic found in the branch office, with the SSG 520 configured to inspect for HTTP “Critical” and DNS “High”, and all HTTP and all DNS signatures, and in both cases with the SSG 520 configured to close malicious sessions. Malicious traffic (Nimda variants and IIS ISAPI exploits) were injected into some tests using the NetworkTester’s stateful replay feature, and the SSG 520 Deep Inspection engine was configured to identify the malicious traffic and close those sessions.

Test Suite 2 Results

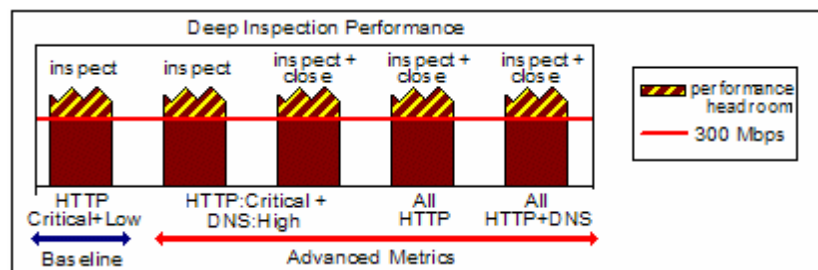
Test Suite 2 established security performance expectations for the SSG, starting with NAT and NAT+Firewall using both 64 byte packets and IMIX traffic profiles. In both the 64-byte tests and the IMIX tests, the SSG 520 significantly exceeded its published baseline datasheet performance metrics. Test Suite 2 also established baseline performance for Deep Inspection using an all-HTTP 64 KB page request traffic profile with the SSG 520 configured to inspect for HTTP “Critical” and HTTP “Low” threats. The 100 background firewall rules, 5 deny rules and NAT functionality remained configured for this test as well. The SSG 520 again significantly exceeded Juniper’s stated 300 Mbps datasheet performance claims for the device.



Once baseline performance values had been established, we proceeded to increase the complexity of the test by adding additional traffic types and simulated threat traffic to the benchmark. The IMIX test scripts were modified to include HTTP, FTP, DNS, and actual attack traffic. Though no longer a “pure” IMIX, the traffic still provides a very real representation of actual branch office traffic, and the test had the added value of real embedded threats that the SSG 520 was required to detect and optionally stop.

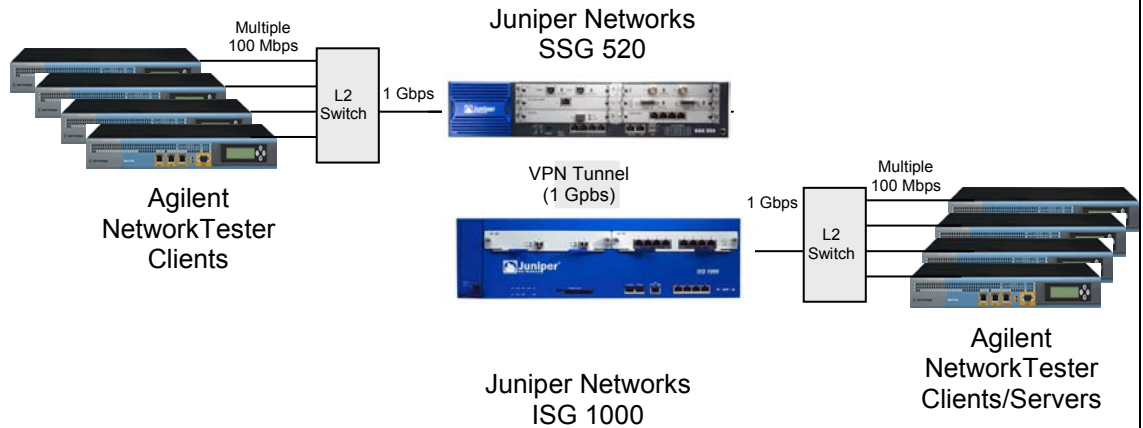
Four tests were run in this configuration. In the first test, the SSG 520 configured to inspect for HTTP “Critical” and DNS “High” threats. In the second test, the SSG 520 was configured to inspect for those threats and close the session of any detected malicious flows. In the third test, the SSG 520 was configured to inspect for all known HTTP attacks, and close any malicious flows, and in the fourth and final test, the SSG 520 was configured to inspect for all known HTTP and DNS attacks, and close any malicious flows.

In the final portion of Test Suite 2, NAT, firewall and Deep Inspection were all enabled. Multi-protocol traffic was used to validate throughput. Increasingly complex configurations using more and more Deep Inspection signatures were tested to validate performance under the most demanding conditions. Finally, actual attack traffic was introduced into the IMIX profile and the firewall was configured to detect and close malicious sessions.



Even under these demanding configuration conditions, which go well beyond Juniper’s recommended configuration settings, the SSG 520 performed as specified, consistently delivering above 300 Mbps of throughput. During tests where the DI attack response of “close” was turned on, the SSG 520 stopped the malicious traffic from traversing the firewall. It is worth noting that Juniper’s datasheet performance claims are for ideal benchmark conditions (e.g. single firewall rule, no NAT, DI with large HTTP requests). Our tests clearly reveal that the SSG 520 has sufficient performance headroom to maintain enterprise-class LAN and WAN performance even with all of the services turned up.

Test Suite 3: Firewall/IPS/NAT+VPN Performance



Test Suite 3 uses a similar methodology and configuration as Test Suite 2, but in this series of tests, the SSG 520 is configured at one end of a site-to-site VPN tunnel. The other end of the VPN is terminated at “corporate headquarters” on a Juniper Networks ISG 1000. The VPN tunnel was configured for 168-bit IPsec 3DES encryption using pre-shared keys and standard IKE negotiation. VPN options were left at interface defaults on the SSG 520 and ISG 1000.

Test Suite 3 begins with a baseline test to provide the reader with results that may be compared to other published industry IPsec benchmarks. This baseline test uses 1,400 byte RTP packets and a single firewall rule “allow all” to measure performance. The use of 1,400 byte packets to measure IPsec performance ensures that the IPsec encrypted packet does not exceed the MTU of the Ethernet interface, which would force packet fragmentation and degrade performance. This benchmark configuration is useful in understanding the best-case performance of an IPsec VPN device, but does not represent the type of traffic likely to be found in a branch office environment.

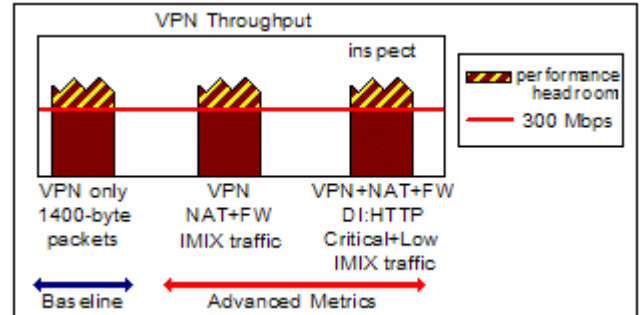
Following the baseline test, IMIX traffic was used to validate the performance of the firewall, NAT, and DI engines while the SSG 520 encrypted traffic through the tunnel. For these tests, the firewall and NAT configuration of the SSG 520 was set to be the same as in Test Suite 2, but a rule to encrypt and tunnel data replaces the “allow all” rule. In this scenario, the SSG 520 had to fragment and reassemble packets on the fly for packets over 1,400 bytes in length.

Two final tests using the modified IMIX with HTTP, FTP, DNS and malicious attack traffic round out Test Suite 3. These final tests represent the worst possible conditions that the SSG 520 might be exposed to in a real branch office environment. The traffic profile used includes a significant amount of large-packet traffic that must be fragmented by the IPsec engine before being encrypted. It also includes the same malicious exploit traffic used in Test Suite 2.

Test Suite 3 Results

Test Suite 3 established security performance expectations for the SSG 520 when providing secure connectivity to a remote site. Juniper claims the SSG 520 can deliver 300 Mbps of encrypted 3DES VPN. While we expected throughput to drop with firewall,

NAT and Deep Inspection functionality enabled, the SSG 520 was able to sustain performance even with all these features enabled. Our benchmarks verified that the SSG 520 can deliver 300 Mbps of throughput not only for 1,400 byte packets, but also when stateful IMIX traffic is used. This series of tests validates that the SSG 520 can deliver sustained performance not only under industry-standard lightweight tests, but also while fielding multi-protocol IMIX traffic requiring fragmentation and reassembly, and demonstrates the power of the dedicated encryption engine in the SSG 520.



Two final tests stress the SSG 520 to its limits with intensive configurations that engage all aspects of the SSG security engine. In these final tests, we enabled first all HTTP signature and then ALL DI signatures the platform will support (software version 5.1 supports 64 total signature sets totaling nearly 1000 threat types). In addition to intensive security scanning, the SSG 520 must provide firewall, NAT and encryption through the IPsec tunnel, and must provide fragmentation and reassembly of packets greater than 1,400 bytes. The SSG 520 Deep Inspection engine was configured to inspect for and close malicious traffic flows.

In these final two tests, we attacked the SSG 520 with the modified IMIX that includes HTTP, FTP, DNS and malicious attack traffic. We finally saw the SSG 520 break a sweat, though the device still performed admirably. The SSG 520 delivered 245 Mbps of throughput with DI set to inspect ALL HTTP (all services were enabled – NAT, Firewall and VPN), and 225 Mbps when all possible DI inspection techniques were turned on. Juniper strongly advises customers not to run under these configurations, because many of the attack inspection types are CPU intensive and are unlikely to be seen in a branch office. However, these tests demonstrate that while performance intensive, the SSG 520 can still deliver well beyond LAN speed performance even when security features are set for maximum defense.

Conclusions

Branch office environments were once designed with best effort throughput in mind. WAN connectivity was handled by the router while security and local connectivity were handled by dedicated firewalls and local LAN switches. Today's mix of enterprise resources in the branch office demand a greater level of segmentation and much higher performance to ensure maximum productivity from branch office workers. Modern technologies are delivering Ethernet-speed WAN links and wireless connectivity, placing greater demands on branch office WAN and security devices than ever before. As these technologies become more pervasive, the demand for high speed security and branch connectivity will only grow.

These test results underscore the scalability and LAN speed performance of the Juniper SSG 520. The benchmarks not only validate the product's data sheet performance, but also underscore the headroom that Juniper has built into its SSG platform, clearly outperforming its conservative data sheet numbers. Even when Fort Knox levels of

security are applied to the SSG 520, performance remains well above the speed of a typical branch office LAN, WAN and wireless network combined. Whether serving as a standalone security solution or as a unified security and WAN access platform, customers can be certain that performance will not be the bottleneck when the SSG 520 is doing the job.

Technical Note – IMIX and Stateful Traffic

IMIX refers to a mixture of packet sizes that approximate the distribution of packets observed on the real Internet. The IMIX distribution is based on the analysis of 342 million packets collected by the National Library for Applied Network Research (NLNR). The analysis revealed that packet sizes on the Internet were largely clustered around three main sizes: 40, 576 and 1,500 byte packets. Benchmarks can accurately reproduce this distribution by generating packets of the corresponding size in a 7:4:1 ratio. Benchmarks which use this “simple IMIX” distribution more accurately represent real-world traffic conditions than simple single-packet-size synthetic benchmarks.

Creating an IMIX traffic distribution using stateful, multi-protocol testing equipment requires the additional step of accounting for the inherent TCP control traffic that a stateful TCP stack generates as part of the transmission process. A packet analyzer was used in conjunction with specially crafted scripts to ensure that the traffic used in this test accurately mirrored the 7:4:1 ratio defined by the “Simple IMIX” profile. More details IMIX are available at http://advanced.comms.agilent.com/n2x/docs/journal/JTC_003.html

Lab Testing Mission Statement

Current Analysis and Iometrix share a common vision to develop rigorous, standards-based methodologies essential to the meaningful evaluation of advanced enterprise and carrier networking equipment. Current Analysis and Iometrix collaborate to develop and execute test methodologies that set new standards for quality and relevance in enterprise and carrier networking equipment testing.

Current Analysis and Iometrix perform independent, commissioned product testing to measure and validate relevant, real-world performance of a product from a single vendor. Testing methodologies are designed and executed exclusively by Iometrix and Current Analysis. Current Analysis and Iometrix share the belief that equipment vendors must be held to a higher level of accountability in lab testing engagements, and together we deliver testing methodologies and benchmarks which are credible and relevant to the end user.

Acknowledgements

Current Analysis and Iometrix would like to specifically thank Agilent Technologies for providing extensive equipment resources, support, development and engineering services throughout the course of this test. Agilent supports the Iometrix lab with its NetworkTester and N2X platforms, and its NetPressure software, which enabled Current Analysis and Iometrix to develop and execute the advanced stateful testing methodologies used in this test.

Current Analysis and Iometrix have made every attempt to ensure that all test procedures were conducted with the utmost precision and accuracy, but acknowledge that errors do occur. Neither Current Analysis nor Iometrix shall be held liable for damages which may result from the use of information contained in this document.