THE TOLLY GROUP

No. 202164 January 2003

WatchGuard Technologies, Inc. Firebox® V60

Competitive Firewall/VPN Benchmark Evaluation Versus Cisco PIX 515E and NetScreen-50

Test Summary

Premise: *When considering the purchase of firewalls and VPN devices, network architects and managers want to validate performance characteristics of available security products. With the growth in high-speed Internet access, users must grapple with the potential performance hit often associated with a secure data path.*

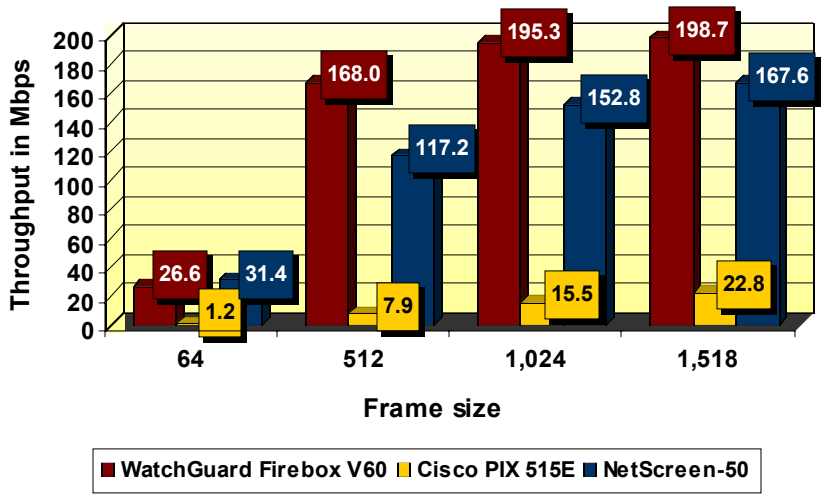
WatchGuard Technologies, Inc. commissioned The Tolly Group to evaluate the Firebox® V60, a four-port Fast Ethernet firewall/VPN security appliance. The Tolly Group subjected the Firebox V60 to a variety of real-world zero-loss throughput scenarios. WatchGuard instructed The Tolly Group to compare the performance of the Firebox V60 against a Cisco Systems Inc. PIX 515E two-port appliance and a NetScreen Technologies Inc. NetScreen-50 four-port appliance. Tests were conducted in January 2003.

Test results show that the Firebox V60 regularly outperformed the Cisco and NetScreen security appliances, delivering up to 21X the firewall throughput of rival appliances tested and almost 190% more VPN throughput in tests of 512-byte frames or higher. Even at the most taxing 64-byte frames, the Firebox V60 performed on par or better than the NetScreen-50 and significantly better than the Cisco PIX 515E.

Test Highlights

- Delivers up to 21X more zero-loss firewall throughput than the Cisco PIX 515E and almost 1.5X the zero-loss throughput of the NetScreen-50 in tests of 512-byte frames and higher with 500 rules enabled
- Achieves up to 188% greater zero-loss VPN throughput of the NetScreen-50 and up to 75% more zero-loss throughput than the PIX 515E in tests of 512-byte frames and higher
- Outperforms the NetScreen-50 for all frame sizes in a real-world firewall configuration of 500 sessions and 500 rules. The Cisco PIX 515E was unable to pass traffic in this test.

Zero-Loss (≤0.001%) Firewall Throughput
2 Fast Ethernet Interfaces, UDP Traffic, 8,000 Sessions, 500 Rules (1-499 Deny - 500 Allow All), NAT Disabled



Source: The Tolly Group, January 2003 *Figure 1*

Results

Firewall Throughput

Tests were conducted in four different scenarios:

- A single rule, "allow all" configuration with network address translation (NAT) disabled. This was the baseline test.

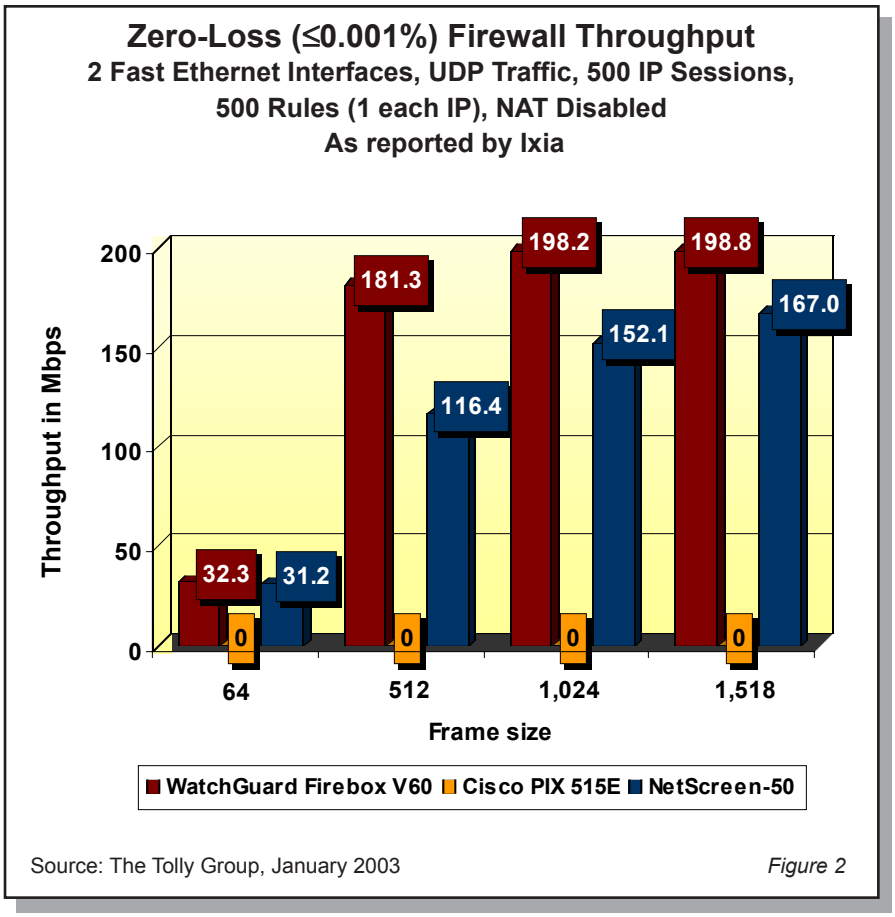
- A single rule, "allow all" configuration with NAT disabled and 8,000 UDP sessions. This simulates traffic from 8,000 users traversing the firewall.

- A scenario with 500 rules (1-499 deny, 500 allow) with NAT disabled and 2, 500 and 8,000 sessions. This test represented a load scenario for the devices under test (DUTs).

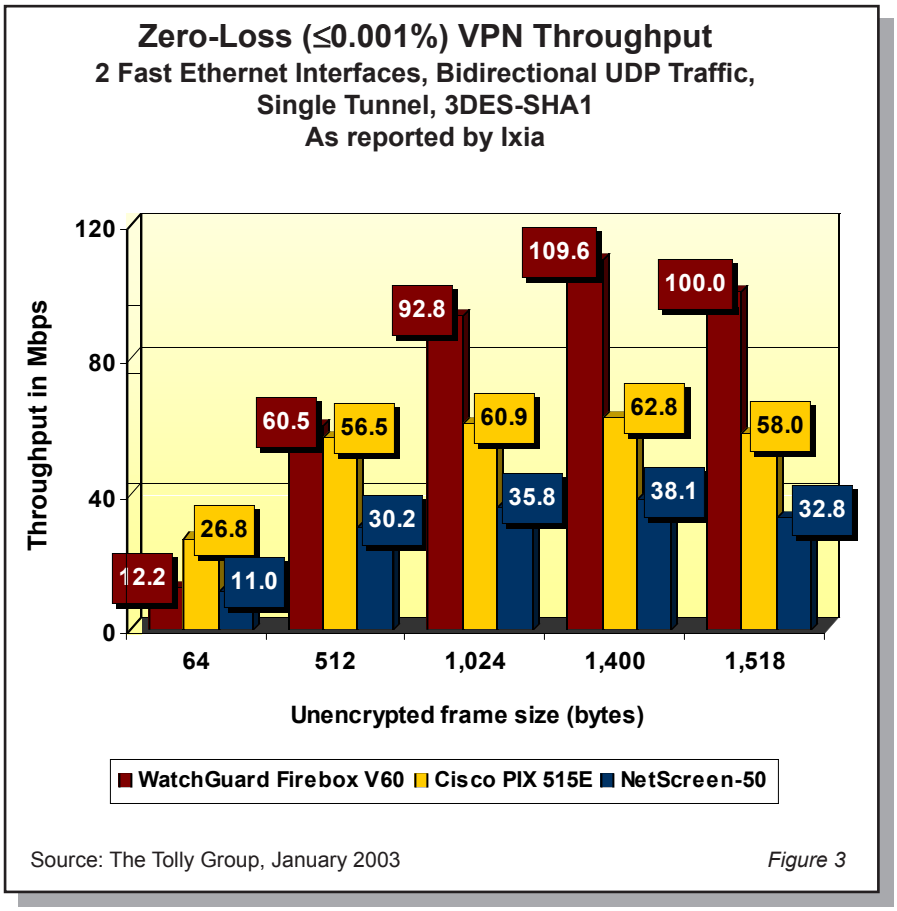
- A scenario with 500 rules (one per each IP address), NAT disabled and 500 IP sessions. This scenario provided a real-world test, approximating traffic between a headquarters location and 50 branch offices or telecommuters, each with a unique IP address and a unique rule.

*(**NOTE**: The term UDP session indicates that the unique session was created by modifying a UDP port number, maintaining a single source/destination IP address pair. The IP session indicates the use of unique IP addresses for each session.)*

In the firewall scenario with 500 rules (1-499 deny, 500 allow) with NAT disabled and 2,500 and 8,000 sessions active, the Firebox V60 forwarded between 27 Mbps and almost 200 Mbps of zero-loss throughput, depending upon frame size (See Figure 1).



Source: The Tolly Group, January 2003 *Figure 2*



Source: The Tolly Group, January 2003 *Figure 3*

When compared to the zero-loss performance of it nearest rival, the NetScreen-50, results show that the Firebox V60 handled from 15% to 30% more traffic when tested at 512-byte frames and higher. The NetScreen 50 yielded between 117 Mbps and 168 Mbps of zero-loss throughput in tests of 512-byte frames and higher. By contrast, the Cisco PIX 515E lagged the field, forwarding between 8 Mbps and 23 Mbps in the same tests at 512-byte frames and higher.

The Firebox V60 maintained its zero-loss firewall throughput lead over the NetScreen and Cisco boxes in a scenario configured with 500 IP sessions and 500 rules (one per each IP address) with NAT disabled. Here, the Firebox V60 outperformed the Cisco and NetScreen products in every packet-size test scenario. In this test, the Firebox V60 forwarded between 181 Mbps and 199 Mbps in tests of 512-byte, 1,024-byte and 1,518-byte packets (See Figure 2). That equates to a zero-loss throughput percentage gain of between 16% and 36% when compared to the NetScreen-50. Even at 64-byte frames, the Firebox V60 forwarded 32 Mbps, or 3% more throughput than the NetScreen-50; during the test timeframe engineers were unable to pass traffic on the Cisco PIX 515E, which subsequently was dropped from the test.

The performance results from both of these "real-world" configurations compares strikingly to the baseline measurements taken for the devices under test. In the zero-loss firewall throughput baseline, engineers ran bi-directional UDP traffic across a single session with one rule (allow all) and NAT disabled. The Firebox V60 forwarded 181 Mbps, 198 Mbps and 199 Mbps for 512-byte, 1,024-byte and 1,518-byte frames, respectively. These baseline results map to the real-world test scenario of 500 IP sessions and 500 rules, in which the Firebox V60 forwarded 181 Mbps at 512-byte frames, 198 Mbps at 1,024-byte frames and 199 Mbps at 1,518-byte frames.

VPN Throughput

With the firewall tests completed, engineers turned their attention to measuring VPN zero-loss throughput. Here, just as in the firewall tests, the Firebox V60 delivered more zero-loss throughput in tests of 512-byte frames and above. In fact, in the VPN throughput tests, the Firebox V60 forwarded 61 Mbps, 93 Mbps, 110 Mbps and 100 Mbps for 512-, 1,024-, 1,400- and 1,518-byte packets (See Figure 3). This represents up to 43% more zero-loss VPN throughput than the Cisco PIX 515E and up to 67% more zero-loss throughput than the NetScreen-50.

Analysis

In terms of firewall throughput in a real-world configuration, the Firebox V60 forwarded up to 21X the zero-loss throughput of the Cisco PIX 515E and almost 1.5X the throughput of the NetScreen-50.

In the real-world test scenario with 500 IP sessions and 500

WatchGuard Technologies, Inc.

Firebox® V60

Firewall/VPN Performance

TOLLY Up to Spec CERTIFIED

WatchGuard Technologies, Inc.
Firebox® V60
Product Specifications*

Features
Performance and Highlights
- 200 Mbps firewall throughput
- 100 Mbps 3DES VPN throughput
- 400 VPN tunnels
- Unlimited user license

Security
- Stateful packet filtering
- Predefined firewall services
- Static, dynamic NAT, Port Forwarding
- Hacker defense for DDoS & DoS prevention
- Port and site blocking
- Firewall user authentication

VPN
- Mobile user and branch office VPN support
- VPN tunnel switching (Hub and spoke)
- Remote access authentication
- PKI X.509 Digital Certificate support
- External RADIUS support

Networking
- High availability
- Multi-tenant security
- 802.1Q VLAN tagging support
- QoS traffic management and traffic port shaping
- Dynamic routing
- PPPoE and DHCP support
- Server load balancing

Management
- Secure Java-based management, CLI, optional central management
- Installation and configuration tools
- Real-time monitoring and notification

Interoperability
- ICSA firewall and IPSec certification
- VPN-compliant

For more information contact:
WatchGuard Technologies, Inc.
505 Fifth Avenue South
Seattle, WA 98104
Phone: (206) 521-8340
URL: http://www.watchguard.com

**Vendor-supplied information not verified by The Tolly Group*

rules, the Firebox V60 throughput increased by an average of 10% over the 500-rule scenario with 8,000 UDP sessions. What makes this interesting is that the NetScreen-50 zero-loss throughput remained flat and the Cisco PIX 515E was unable to handle the real-world test.

Moreover, the Firebox V60 throughput results were consistent across the test scenarios and most closely resembled the "best-case" throughput generated in the baseline test when compared to the Cisco and the NetScreen products even under the duress of heavy loads. In fact, in the "real-world" test of 500 IP sessions with 500 rules, the Firebox V60 throughput mapped almost identically to the packet test performance achieved in the baseline tests.

Testing also was designed to demonstrate the impact of having multiple rules active on the device. For this testing, two succinctly different rule sets were used. In the first configuration, the first 499 rules were configured to deny all traffic and the 500th rule was to allow all traffic. In the second configuration, each of the 500 rules was directly related to a unique flow, forcing the DUTs to exercise all rules.

The 8,000 UDP sessions testing with 500 rules, where the first 499 rules denied all traffic and the 500th allowed all yielded results that mimicked those obtained with 8,000 UDP sessions and 1 rule, with the exception of WatchGuard where the Firebox V60 lost less than 1 Mbps of throughput when tested with 64- and 1,024-byte packets and 6.6 Mbps of throughput when tested with 512-byte frames. The Cisco PIX 515E, meanwhile, lost more than 3 Mbps of throughput when tested at 512-byte packets.

Modifying the rule set so that each of the 500 rules corresponded to a specific IP session had a positive effect on the Firebox V60 device with the 64-byte and 512-byte frames. Results increased by almost 6 Mbps to 32 Mbps, or 21%, on the 64-byte and by 13.3 Mbps to 181 Mbps, or 8%, on the 512-byte frames. Engineers were unsuccessful at configuring the Cisco PIX 515E to pass traffic successfully in this configuration and therefore it is omitted in the results.

On the VPN side, the Firebox V60 again demonstrated consistent performance. At 512-byte packets the Firebox V60 passed slightly more than 30% of the theoretical maximum, compared to the NetScreen-50, which was capable of only passing 15%, while the Cisco PIX 515E forwarded 28% of the theoretical maximum. At 1,024-byte packets, the Firebox V60 forwarded 46% of the theoretical maximum zero-loss throughput while the PIX 515E reached only 30% and the NetScreen-50 achieved only 18%. At 1,400-bytes, one of the largest non-fragmenting frame sizes, engineers observed the largest performance delta with the Firebox V60 forwarding 55% of zero-loss throughput with the PIX 515E and the NetScreen-50 obtaining 31% and 19% respectively.

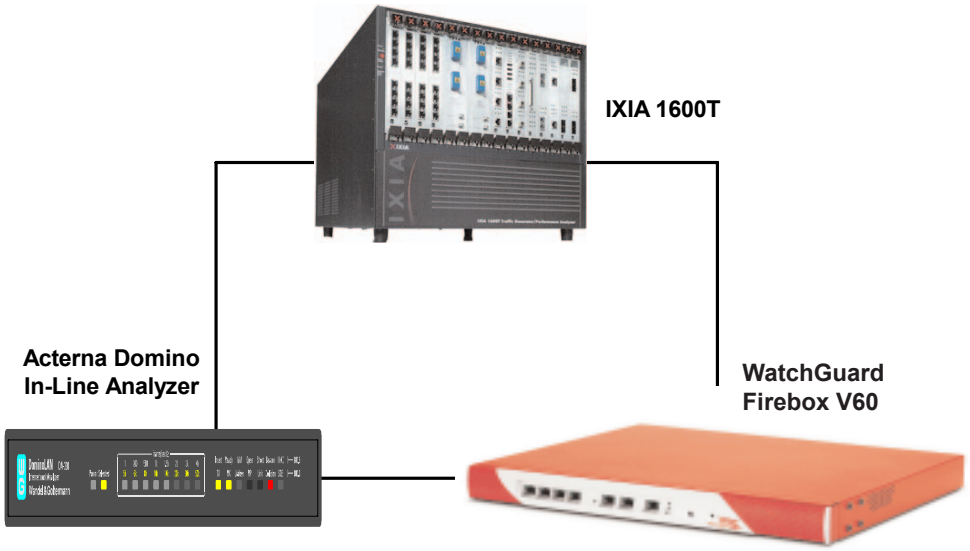
Testing of the 1,518-byte packet provided insight into the test devices' capability to fragment and forward maximum Ethernet frame sized packets. Fragmentation occurs when the added IPSec header creates a packet larger than the maximum allowable Ethernet frame size of 1,518 bytes. The packet is broken into two smaller packets, one large and one small and are both encapsulated in an IPSec packet with the responsibility of either the far-side DUT or the end station to reassemble the packet.

Our testing determined that Firebox V60 and NetScreen-50 both performed packet reassembly while the Cisco PIX 515E forwards fragmented packets leaving the responsibility for reassembly with the client end station. Because of the way Cisco handles fragmentation, a special Ixia configuration needed to be created which took into account the counting of the fragmented packets only (large and small) and did not take into account sequence numbers. WatchGuard performed at 50% of the theoretical maximum, with Cisco recording 29% and NetScreen recording 16%.

Test Configuration and Methodology

The Tolly Group tested a WatchGuard Technologies Firebox V60 version 4.0 Fast Ethernet firewall/VPN appliance to measure the device's zero-loss firewall throughput and zero-loss VPN throughput. Tolly Group engineers tested the firewall/VPN performance of the Firebox V60 against a Cisco Systems, Inc. PIX 515E OS 6.1.4 and a NetScreen Technologies NetScreen-50 Version 4.0.1 R2.

Firewall Test Bed



Source: The Tolly Group, January 2003

Figure 4

For firewall tests, the devices under test (DUTs) were evaluated for their steady-state zero-loss packet per second (PPS) throughput using different packet sizes (64, 512, 1,024 and 1,518 bytes) on a firewall with fully populated interfaces.

For each test, the DUTs were connected in a Fast Ethernet configuration to an IXIA 1600T, which generated test traffic (See Figure 4). DUTs were configured for the different traffic scenarios as previously described in the Firewall results section. Engineers configured the Ixia ScriptMate software to execute the test according to defined load and configurations. For the 8,000-session test, session timeouts were set to the maximum threshold. All sessions were configured and established prior to running the test. The Ixia ScriptMate reported results and adjusted the offered load in 1% decrements starting at 100% of the theoretical load until the zero-loss rate was established. An Acterna Domino in-line analyzer was used to confirm packet sizes in use during prototype testing; the device was removed prior to production testing.

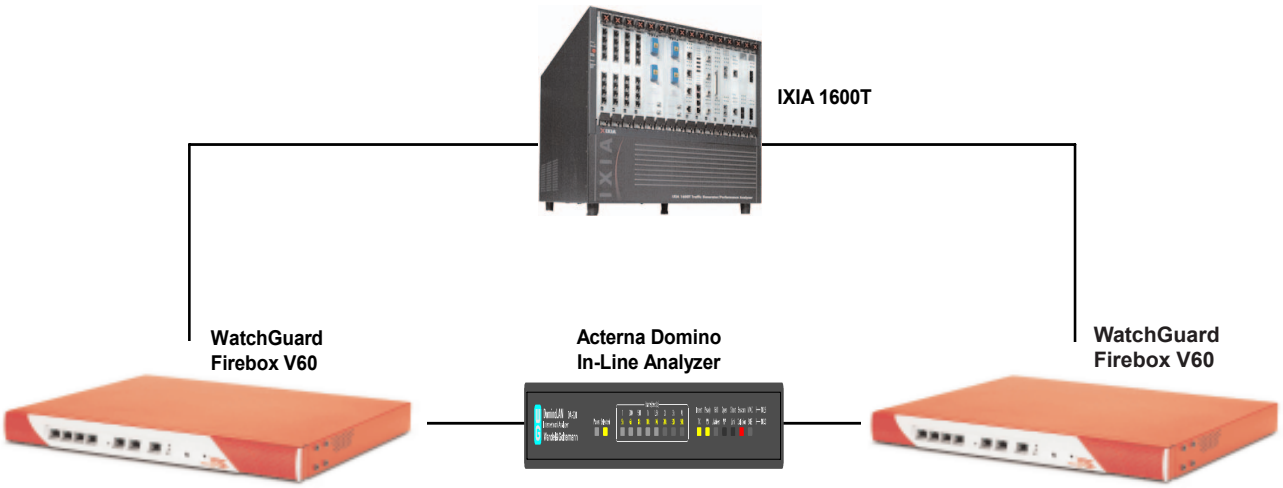
On the VPN side, engineers benchmarked the steady state, zero-loss PPS throughput using different packet sizes (64, 512, 1,024, 1,400 and 1,518 bytes) on an IPSec gateway pair.

Engineers connected all appropriate networking infrastructure (DUT console, Ixia console, Ixia interfaces, DUT interfaces). (See Figure 5.) Then, they configured a pair of DUTs to encrypt/decrypt and authenticate traffic from each trusted network.

Engineers also configured Ixia ScriptMate to execute the test at the appropriate load and configurations as specified. Ixia ScriptMate recorded the results and adjusted the offered load in 1% decrements starting from 100% of the theoretical maximum.

Engineers used a Domino NAS 2.0 (Domino Core 3.0) to confirm correct packet size, validate encrypted traffic where appropriate and network utilization.

VPN Test Bed



Source: The Tolly Group, January 2003

Figure 5

The Tolly Group gratefully acknowledges the providers of test equipment used in this project.

Vendor	Product	Web address
Ixia Communications	IXIA 1600	http://www.ixiacom.com
Ixia Communications	IXIA ScriptMate	http://www.ixiacom.com
Ixia Communications	IXIA IxExplorer	http://www.ixiacom.com

Tolly Group Services

With more than a decade of testing experience of leading-edge network technologies, The Tolly Group employs time-proven test methodologies and fair testing principles to benchmark products and services with the highest degree of accuracy. Plus, unlike narrowly focused testing shops, The Tolly Group combines its vast technology knowledge with focused marketing services to help clients better position product benchmarks for maximum exposure. The company offers an unparalleled array of reports and services including: Test Summaries, Tolly Verifieds, performance certification programs, educational Webcasts, white paper production, proof-of-concept testing, network planning, industry studies, end-user services, strategic consulting and integrated marketing services. Learn more about The Tolly Group services by calling (732) 528-3300, or send E-mail to info@tolly.com.

For info on the Fair Testing Charter, visit: www.tolly.com/About/ftc.asp

Project Profile

Sponsor: WatchGuard Technologies, Inc.

Document number: 202164

Product Class: Network security appliance

Products under test:

- WatchGuard Firebox V60 Version 4.0
- Cisco Systems, Inc. PIX 515E OS 6.14
- NetScreen Technologies NetScreen-50 Version 4.0.1 R2

Testing window: January 2003

For more information on this document, or other services offered by The Tolly Group, visit our World Wide Web site at http://www.tolly.com, send E-mail to info@tolly.com, call (800) 933-1699 or (732) 528-3300.

The Tolly Group doc. 200164 rev. dto 25 Feb 03