THE TOLLY GROUP

No. 201130 July 2001

Nortel Networks, Inc.

Contivity 2600 VPN Switch

Firewall/VPN Multi-Service Performance Evaluation

Test Summary

Premise: *Buyers of enterprise-class VPN/firewall devices need to consider how these devices fit into their LAN/WAN infrastructure to ensure they adequately perform their enterprise mission. Performance of such devices is tied hand-in-hand to the processing overhead imposed by the encryption and the security screening services they deliver. Network designers accustomed to wire-speed network LAN infrastructure need to be sure that overall network performance will not suffer when implementing a device providing both security and encryption of sensitive information.*

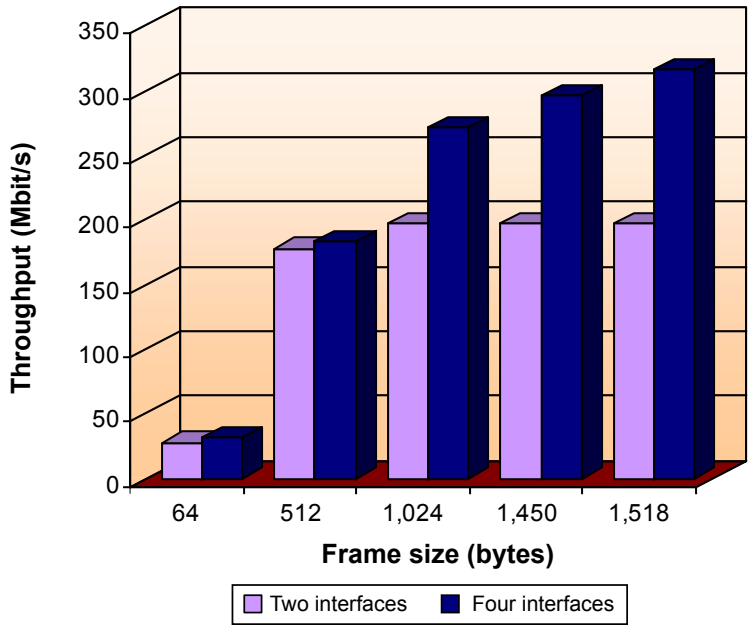
Nortel Networks, Inc. commissioned The Tolly Group to evaluate its Contivity 2600, the mid-range member of the Contivity VPN Switch family. The Contivity 2600 is designed to serve large branch offices or data centers that support up to 1,000 VPN tunnels. Tolly Group engineers subjected the Contivity 2600 to a battery of tests to determine the switch's single-rule firewall and IPSec gateway bidirectional zero-loss performance, as well as benchmark switch performance when both services are vying for bandwidth. Testing was conducted during June and July 2001.

Overall, test results show that the Contivity 2600 achieves high-throughput for stand-alone stateful inspection firewall service – more than enough to serve a majority of an enterprise's branch, regional or headquarters' throughput needs. The Contivity 2600 also demonstrated more than sufficient throughput when running a combination of VPN and stateful inspection firewall traffic, with zero frame loss.

Test Highlights

- Delivers up to 316 Mbit/s of bidirectional zero-loss throughput when handling 1,518-byte frames across two port-pairs in a firewall configuration
- Achieves up to 112 Mbit/s of bidirectional zero-loss throughput handling 1,518-byte frames in a VPN IPSec gateway scenario with 3DES and SHA-1
- Provides 190 Mbit/s of firewall throughput while simultaneously passing 80 Mbit/s of 3DES, SHA-1 and IPSec traffic

Single-Rule Firewall, Zero-Loss Throughput
SmartBits Bidirectional Traffic,
UDP Frames over Full-Duplex Fast Ethernet



Source: The Tolly Group, July 2001

Figure 1

Results

Single-rule firewall bidirectional zero-loss throughput

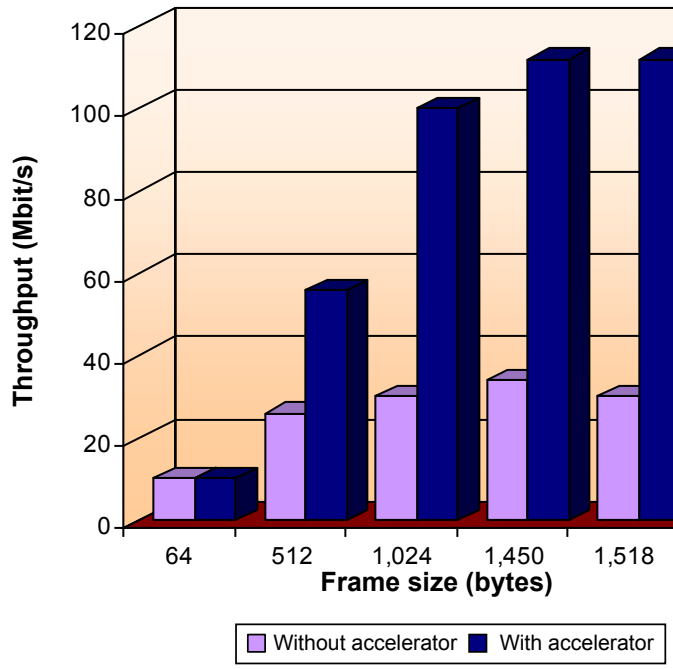
The tests examined a Contivity 2600 configured as a "single-rule" firewall with throughput measurements taken in scenarios using a single port-pair and dual port-pair. For the single port-pair test, the single-rule firewall was configured in a full-duplex Fast Ethernet environment with a single client IP address on the public side of the firewall transmitting and receiving traffic to/from a single client IP address on the private side. The dual port-pair test was similarly configured to the two-port test, but with double the port density.

The single port-pair test demonstrated that the Contivity 2600 achieved a zero frame-loss level of 99% for 1,024-, 1,450-, and 1,518-byte frames, based upon theoretical maximum frame rate; this corresponds to a 198 Mbit/s throughput rate. UDP traffic was sent bidirectionally.

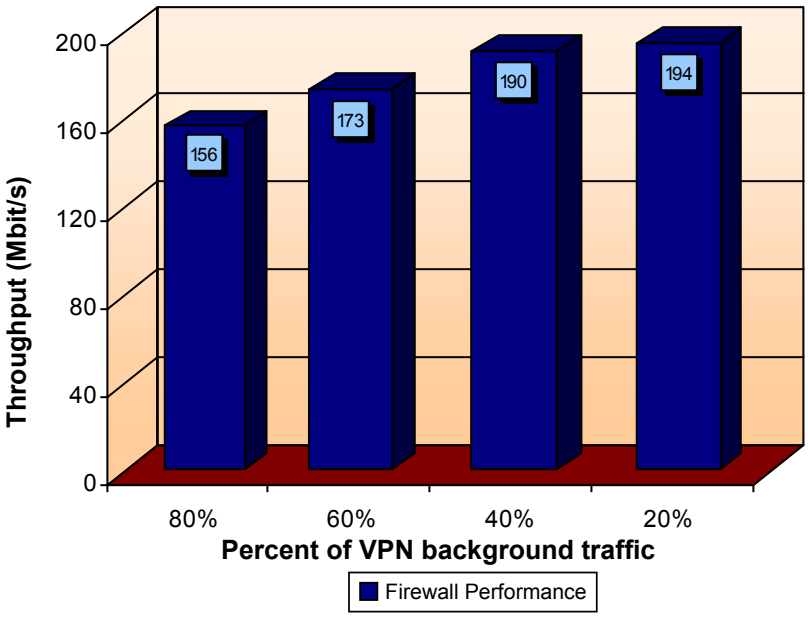
The dual port-pair tests demonstrated that the Contivity 2600 achieved a zero frame-loss level of 79% for 1,518-byte frames, based upon theoretical maximum frame rate; this corresponds to a 316 Mbit/s throughput rate (see Figure 1).

IPSec gateway bidirectional zero-loss performance

For this evaluation process, a VPN tunnel was created between a pair of IPSec gateways. The IPSec protocol adds approximately 50 bytes of header information to a single frame upon transport, therefore exceeding the IEEE 802.3 Ethernet standard frame size of 1,518 bytes. This causes fragmentation, which can impact throughput severely. However, the Contivity 2600 performance maintains high throughput rates even with fragmentation.



Source: The Tolly Group, July 2001 *Figure 2*



[1] Firewall throughput was derived by benchmarking the Contivity 2600 in the presence of varying percentages of VPN background traffic.

Source: The Tolly Group, July 2001 *Figure 3*

Tests were performed both with and without an accelerator device installed in the Contivity 2600; the accelerator device offloaded encryption/decryption processing from the core processor of the system under test.

Tests showed that Contivity 2600 functioning as an IPSec gateway without an accelerator installed operated at a throughput level of 30 Mbit/s to 34 Mbit/s for 1,024-, 1,450-, and 1,518-byte frames (see Figure 2). In contrast, when similar tests were conducted with an accelerator installed, the Contivity 2600 operated at a throughput level of 100 Mbit/s to 112 Mbit/s for 1,024-, 1,440-, and 1,518-byte frames, more than a 300% increase. Traffic was sent bidirectionally and all measurements were of the unencrypted source frames.

Multi-service bidirectional zero-loss performance

For this test, the Contivity 2600 supported firewall and VPN functions simultaneously. The VPN input was maintained at a predetermined frame-per-second level (as a percentage from previous baseline testing), while the firewall input was incremented/decremented until the switch achieved a zero-loss level. All parameters that were used for previous firewall and VPN baseline tests remained, including the exclusive use of the VPN accelerator.

Nortel Networks, Inc.

Contivity 2600 VPN Switch

Functionality and Performance

Tests showed that Contivity 2600, functioning as a multi-service device with both the single-rule firewall and IPSec gateway with an accelerator installed, operated at up to 194 Mbit/s (equal to 87% of its theoretical maximum firewall throughput for 1,518-bytes frames) at the same time

Nortel Networks, Inc.
Contivity 2600
Product Specifications*

Tunneling protocols
- IPSec, including authentication header (AH), encapsulating security protocol (ESP), and Internet key exchange (IKE); PPTP, including compression and encryption; L2F and L2TP

Routing Protocols
- RIP v1, RIP v2, OSPF and VRRP

Authentication services
- LDAP and RADIUS
- Token card integration: Security Dynamics and AXENT, e.g. SecureID
- Digital certificate with Entrust, Verisign; Microsoft, Netscape, Baltimore Technologies and RSA Keon
- Smart Card integration via MS-CAPI

Encryption
- FIPS 140-1 Level 2 certified
- IPSec-certified by the ICSA
- DES, 3DES and RC4

Filtering criteria
- Individual user or group profile; source and destination IP address; port, service, and protocol type; synchronize flag/acknowledgement (SYN/ACK) bit

Bandwidth management
- Group-level minimum bandwidth settings, priority levels using RED; four admission control levels; four forwarding priority levels; eight DiffServ queues; code point marking; QoS, and RSVP

Accounting
- Internal and external RADIUS accounting
- Event, system, security and configuration accounting
- Automatic archiving to external system

Management
- Full HTML and Java configuration; SNMP alerts; bulk load configuration; NNCLI; role-based management
- Optivity NCS for management of multiple Contivity switches
- IP VPN Service Management Solution

Security
- Contivity stateful firewall, including stateful packet inspection and audit
- Network address translation (NAT), NAPT and NAT Traversal

Client software
- Supports Windows 95, 98, 2000, Millennium, or Windows NT** 4.0 or later; Macintosh OS
- IPSec, including AH, ESP, IKE, third-party main and aggressive-mode clients
- Auto-configuration with "one-click" connection

For more information contact:

Nortel Networks
8200 Dixie Road
Brampton, Ontario L6T 5P6
Canada
Phone: 1-800-4-NORTEL (1-800-466-7835)
URL: http://www.nortelnetworks.com

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

the switch was handling 20% of the baseline VPN traffic generated in a previous test (see Figure 3).

When engineers increased the VPN load up to 80% utilization of the baseline load, the Contivity 2600 achieved a zero-loss throughput of 157 Mbit/s (or 40% of the firewall's theoretical maximum throughput). All traffic was sent bidirectionally and all measurements were of the unencrypted source frames.

Analysis

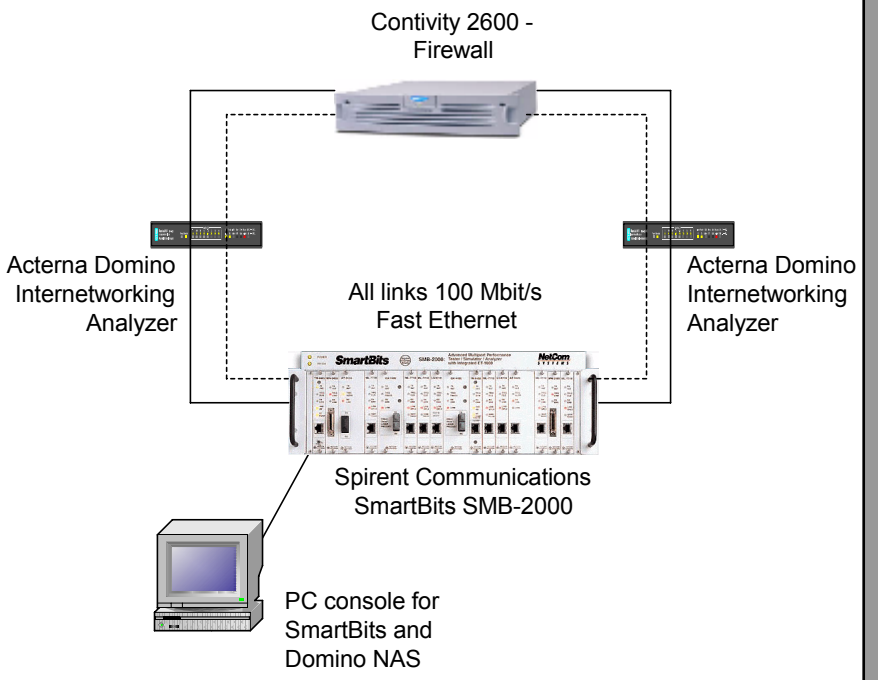
In the past, firewall and VPN technologies, when introduced to unprotected networks, have exacted a substantial penalty in terms of reduced throughput. Filtering, inspection, cryptography – each play a role in bringing down the effective throughput to a range associated with ordinary Ethernet. Although software-based firewall and VPN solutions have been employed widely, maintaining the throughput levels of unprotected networks is best achieved by employing hardware-based solutions.

The Contivity 2600 employs a hardware-based solution that provides the level of security modern networks require and at the same time maintains a level of throughput comparable to unsecured networks.

Test results indicate that the Contivity 2600 provides more than the expected encryption, decryption, and authentication support functions while still supplying the type of throughput rates required for secure enterprise-scale traffic volume and application loads within a campus and/or metropolitan area network (MAN) using Fast Ethernet technology.

Testing also demonstrates that the Contivity 2600 simultaneously can provide both the stateful firewall and 3DES IPSec performance to support MAN networks requiring full-duplex 10/100 Mbit/s throughput.

Single-Rule Firewall Test Bed



Source: The Tolly Group, July 2001 *Figure 4*

Test Configuration and Methodology

IPSec Tunnel Test Bed Configuration

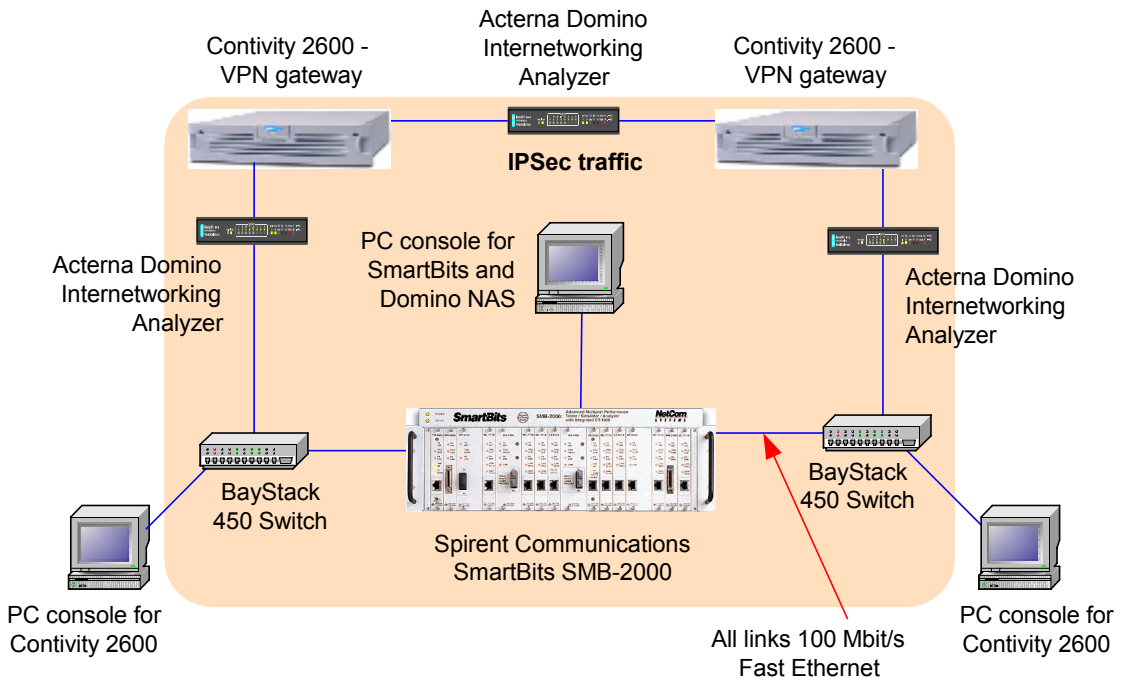
For IPSec tunnel performance tests, engineers connected a pair of Nortel Networks, Inc. Contivity 2600 VPN Switches, v03_65.02, with accelerator cards, to each other via full-duplex, Fast Ethernet. Each of the Contivity 2600s, configured as IPSec gateways, was connected to a Nortel Networks BayStack 450-24T 24-port Ethernet Switch hardware version, Rev L, firmware version vl.47, software version. v3.1.0.22. An Acterna DominoPlus DA-360 hardware-based network analyzer running DominoCore software version 3.0 configured for 100Base-TX full duplex sat in-line between the Contivity 2600s. Two identical DominoPlus DA-360 network analyzers were configured in-line between each pair of devices and each Nortel BayStack switch.

Each BayStack switch also connected to a Spirent Communications SmartBits SMB-2000 Advanced Multiport Performance Tester/Analyzer/Simulator, firmware version 6.63.0004, equipped with six ML-7710, 10/100 Mbit/s Ethernet interfaces.

The SmartBits console ran Spirent SmartWindows 7.0026. This PC ran Microsoft Windows NT WorkStation 4.0 SP5.

IPSec Tunnel Test Methodology

Tests were conducted with a Contivity 2600 operating as a VPN/IPSec gateway using Data Encryption Standard-3 (3DES), an encryption algorithm utilizing three separate keys forming an effective key length of 168-bits, and Secure



Source: The Tolly Group, July 2001

Figure 5

Hashing Algorithm 1 (SHA-1), an authentication technology that includes a hash function that verifies that frames sent have not been changed.

Tolly Group engineers tested the systems under test in IPSec tunnel configurations for zero-loss throughput. All traffic was encrypted for 3DES with a shared secret key and SHA-1. For steady-state, zero-loss, bidirectional frame-per-second tests, engineers measured the frame loss of the Contivity 2600 when offering 100% of the theoretical maximum load and adjusted the offered load in 1% decrements until zero-loss was achieved. SmartBits generated 64-byte to 1,518-byte UDP frames. Engineers ran three iterations of each frame size for 60 seconds. The DominoPlus DA-360 devices that were outside the IPSec tunnel verified frame sizes and utilization. The DominoPlus DA-360 configured in-line with the IPSec tunnel verified the encapsulation of each frame. SmartBits measured the percent of traffic forwarded by the tunnel under test.

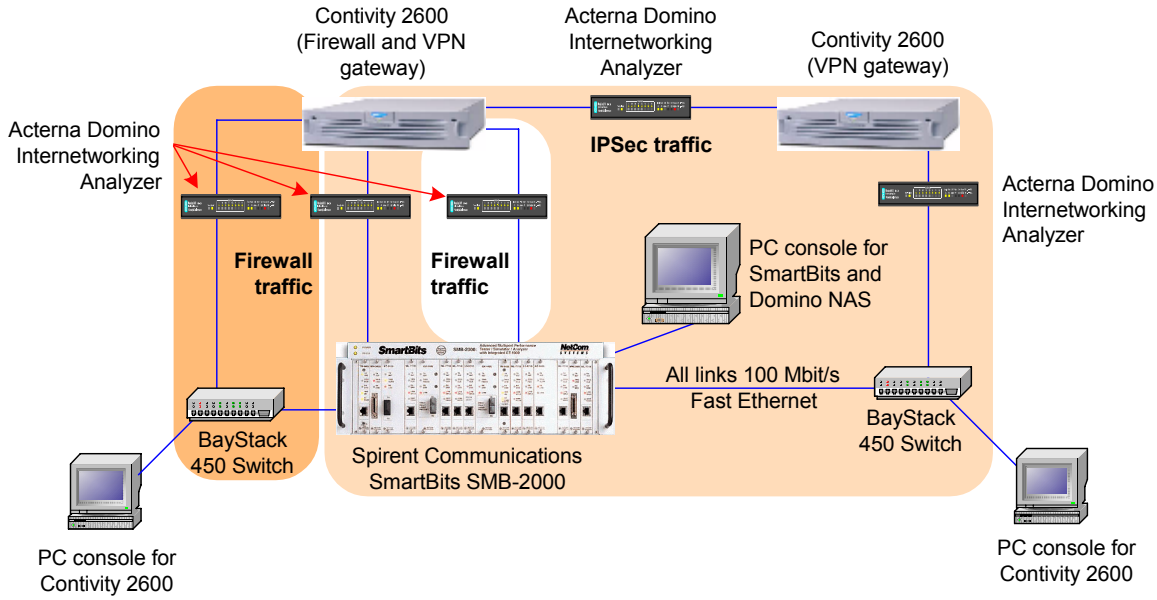
Firewall Test Bed Configuration and Methodology

For firewall throughput tests, engineers removed one of the devices under test from the test system and the DominoPlus DA-360 located in between these appliances. Engineers then configured the device under test as a single rule, allow-all firewall with Network Address Translation (NAT) in idle mode. The remaining test bed was the same as the IPSec tunnel test bed. The Tolly Group engineers measured the percent of traffic the device forwarded when offered 100% of the theoretical maximum load. SmartBits generated 64- to 1,518-byte UDP frames. SmartBits measured the percent of traffic forwarded by the firewall under test. The two DominoPlus DA-360 devices that were on either side of the firewall verified frame sizes and utilization.

Multi-service test bed configuration and methodology

For multi-service tests, engineers configured one of the pair of devices under test in the IPSec tunnel configuration as a single-rule, pass-all firewall in addition to its being configured as a VPN gateway and added two additional Domino DA-360s in-line between the newly configured device under test and the SmartBits console. The remaining test bed was identical to the IPSec tunnel test bed. SmartBits generated 64-byte to 1,518-byte UDP frames. Engineers determined firewall throughput in the presence of various IPSec tunnel loads of 20%, 40%, 60% and 80% of the baseline IPSec throughput achieved in earlier tests. The baseline IPSec results, in effect, served as measured loads against which engineers measured firewall performance. All traffic was bidirectional and all measurements were of the unencrypted source frames.

Multi-Service Test Bed



Source: The Tolly Group, July 2001

Figure 6

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

Vendor	Product	Web address
Acterna Corp.	DominoPlus DA-360	http://www.acterna.com
Acterna Corp.	DominoCore	http://www.acterna.com
Spirent Communications	SmartBits SMB-2000	http://www.spirent.com
Spirent Communications	SmartWindows	http://www.spirent.com

TESTED SmartBits

TOLLY FAIR TESTING CHARTER

Since its inception, The Tolly Group has produced high-quality tests that meet three overarching criteria: All tests are objective, fully documented and repeatable.

We endeavor to provide complete disclosure of information concerning individual product tests, and multiparty competitive product evaluations.

As an independent organization, The Tolly Group does not accept retainer contracts from vendors, nor does it endorse products or suppliers. This open and honest environment assures vendors they are treated fairly, and with the necessary care to guarantee all parties that the results of these tests are accurate and valid. The Tolly Group has codified this into the Fair Testing Charter, which may be viewed at http://www.tolly.com.

Project Profile

Sponsor: Nortel Networks, Inc.
Document number: 201130
Product class: VPN appliance with firewall and IPSec gateway functionality
Products under test:
- Contivity 2600 VPN Switch

Testing window: June and July 2001
Software versions tested:
- Version 03_65.02

Software status:
- Generally available

Additional information available:
- Technical Support Diaries
- Configuration Files
- Data Files

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. 201130 rev. clk 10 Oct 01