THE TOLLY GROUP

No. 205147 December 2005

Future Systems, Inc.

FSC2003 SoC (System on a Chip) in Future Systems RenoGate, a SOHO Firewall and VPN Appliance

FSC2003 SoC Firewall and VPN Performance Evaluation using RenoGate

TOLLY 16 YEARS 1989-2005 Test Summary

Premise: *As the deployment of firewall and VPN technologies has been an inevitable trend for all big companies, broadband internet connection without security puts high risks on their computers and private data. A residential/SOHO gateway, which operates as a firewall, a VPN gateway or mixture of multi-functions, appears to be a strong safeguard. Keeping your home or office secure, the SOHO gateway must not be a bottleneck of the network performance and should have sufficient processing power available for ever-evolving networks.*

Future Systems, Inc. commissioned The Tolly Group/TTA (Telecommunications Technology Association) to evaluate its FSC2003 System on Chip (SoC) residing in RenoGate, a Fast Ethernet firewall and VPN appliance.

TTA/TTG benchmarked the bi-directional steady-state zero-loss (≤ 0.001%) firewall and VPN throughput across two Fast Ethernet interfaces when RenoGate equipped with FSC2003 SoC operated as a firewall or a VPN gateway respectively.

Firewall throughput was measured for 1 and 500 firewall rules, for 10 and 100 UDP sessions when RenoGate operated in Layer 2 or Layer 3 mode. The firewall throughput was measured for 64-, 128-, 256-, 512-, 1,024-, 1,400- and 1,518-byte Ethernet frame sizes generated by Spirent Communications SmartBits SMB-600 (Testing S/W: SmartFlow 4.5) equipped with two Fast Ethernet interfaces.

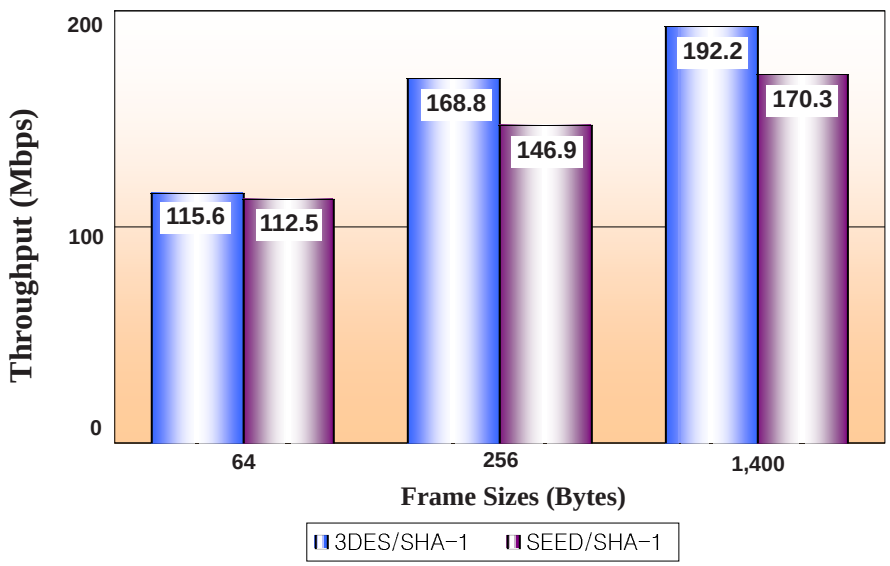
For the IPSec VPN throughput testing, engineers tested two different encryption methods (3DES and SEED) for the frame sizes of 64, 256, and 1,400 bytes. Three RenoGates were configured to establish

Test Highlights

- Delivers 192 Mbps and 170 Mbps of bi-directional, zero-loss (≤0.001%) IPSec VPN throughput for 1,400-byte frame size using 3DES/SHA-1 and SEED/SHA-1 respectively
- Achieves 100% of theoretical maximum firewall throughput (across two Fast Ethernet interfaces) when tested with all frame sizes in a scenario with up to 500 rules and 100 sessions in bridge mode
- Achieves 100% or nearly 100% of theoretical maximum firewall throughput (across two Fast Ethernet interfaces) when tested with all frame sizes in a scenario with up to 500 rules and 100 sessions in router mode tested with 64-byte frames in Layer 3 mode

Zero-loss (≤0.001%) Aggregate VPN Throughput Across Future Systems RenoGate in Dual-Tunnel Configuration

As reported by SmartBits SmartFlow 4.5



VPN Configuration : Gateway-to-Gateway, Tunnel mode

Source: TTA/The Tolly Group, December 2005 *Figure 1*

two separate VPN tunnels where a nominal RenoGate initiated each VPN tunnel to the other two.

Results

VPN: 3DES/SHA-1 & SEED/SHA-1 Bi-directional Zero-Loss Throughput

RenoGate equipped with FSC2003 SoC forwarded up to 96% of the theoretical maximum throughput through dual Fast Ethernet IPSec tunnels using the 3DES/SHA-1 scheme for the frames sizes of 64, 256 and 1,400 bytes. Engineers also found that RenoGate forwarded up to 85% of the theoretical maximum throughput through dual Fast Ethernet IPSec tunnels using SEED/SHA-1. (See Figure 1.)

Engineers configured three RenoGates to serve as an IPSec VPN gateway that uses 3DES/SHA-1 or SEED/SHA-1 as the encryption and authentication method. Engineers measured the bi-directional zero-loss ($\leq$ 0.001%) throughput across two VPN tunnels with Fast Ethernet interfaces configured as full-duplex.

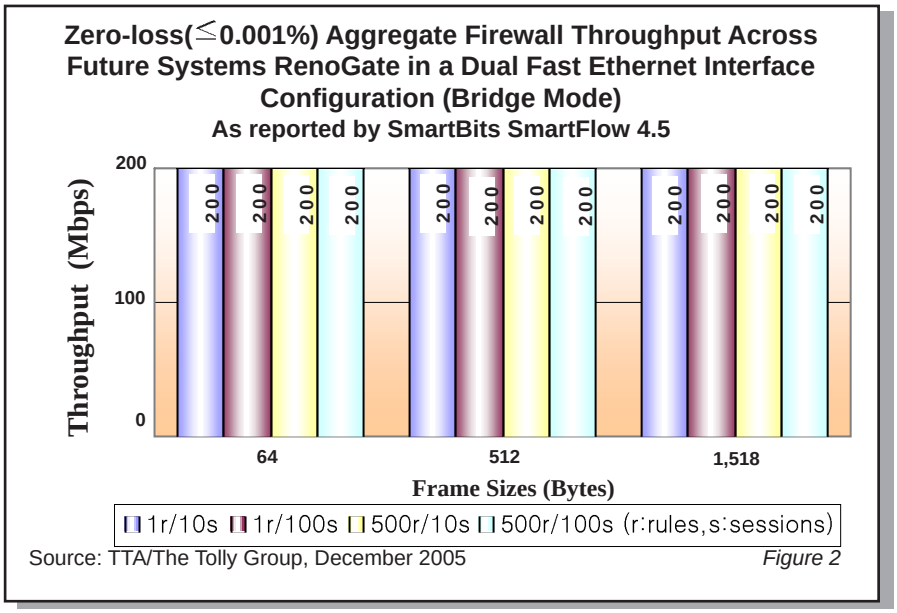
For the 3DES/SHA-1 scheme with a dual tunnel configuration, RenoGate equipped with FSC2003 SoC processed the bi-directional 115.6 Mbps throughput for 64-byte, 168.8 Mbps for 256-byte, and 192.2 Mbps for 1,400-byte frames. For the SEED/SHA-1 scheme with a dual tunnel configuration, RenoGate forwarded the bi-directional 112.5 Mbps throughput for 64-byte, 146.9 Mbps for 256-byte, and 170.3 Mbps for 1,400-byte frames.

Firewall: Layer 2/Layer 3 Bi-directional Zero-Loss Throughput

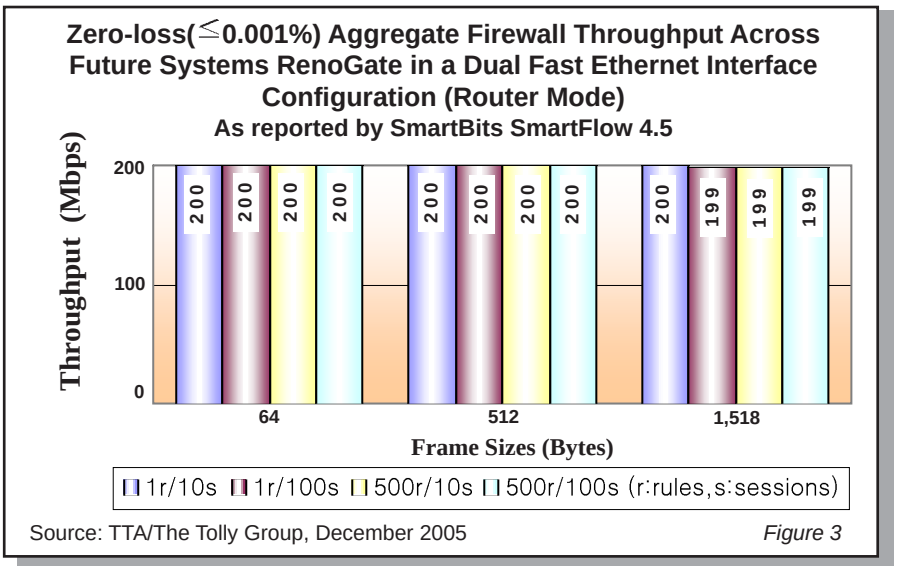
The test results proved that RenoGate equipped with FSC2003 SoC showed wire-speed performance in Layer 2 and Layer 3 firewall mode for most test cases. (See Figures 2 & 3.)

First, engineers configured RenoGate to serve as a Layer 2 (Bridge mode) firewall mode with a single rule or 500 rules according to test cases. Engineers measured the bi-directional zero-loss ($\leq$ 0.001%) throughput across a firewall with two Fast Ethernet interfaces configured as full-duplex mode. Engineers set up the SmartBits to generate test traffic consisting of 10/100 UDP sessions according to test cases and frame sizes of 64, 128, 256, 512, 1,024, 1,400 and 1,518 bytes. When handling any sizes of frames with either a single rule or 500 rules, the RenoGate equipped with FSC2003 SoC delivered 200 Mbps of zero-loss ($\leq$ 0.001%) aggregate firewall throughput for 10 and 100 UDP sessions.

Next, engineers configured the RenoGate to run in a Layer 3 (Router mode) firewall mode with a single rule or 500 rules according to test cases. Engineers also measured the bi-directional zero-loss ($\leq$ 0.001 %) throughput across a firewall with Fast Ethernet interfaces configured as full-duplex mode. When handling all sizes of frames except 1,518 bytes regardless of 1 or 500 rules tested, the RenoGate delivered the bi-directional 200 Mbps throughput for 10 and 100 UDP sessions. When handling 1,518-byte frames with a single rule, the RenoGate delivered 200 Mbps of aggregate firewall throughput for 10 UDP sessions and 198.8 Mbps for 100 UDP sessions. When handling 1,518-bytes frames



Source: TTA/The Tolly Group, December 2005 *Figure 2*



Source: TTA/The Tolly Group, December 2005 *Figure 3*

with 500 rules, the RenoGate delivered 198.8 Mbps of aggregate throughput for both 10 and 100 UDP sessions.

Analysis

FSC2003 SoC aims at enhancing the performance of packet handling functions including filtering and data security. In order to measure easy-to-understand capabilities of the FSC2003 SoC, engineers tested Future Systems', SOHO gateway product, RenoGate equipped with FSC2003. The test has proved that with the help of Future Systems FSC2003 SoC, RenoGate provides near wire-speed throughput performance when it is configured as a firewall or an IPSec VPN gateway.

The RenoGate equipped with FSC2003 SoC supports IPSec VPN functionality. IPSec VPN gateway enables users to establish secure communication channels over public IP networks. In order to gain security over publicly open networks, it normally hides the contents of IP packets by a variety of encryption methods, and then retrieves the original contents by decryption. Among the encryption and authentication methods that RenoGate supports, engineers performed the maximum throughput tests for both 3DES/SHA-1 and SEED/SHA-1 modes.

In VPN throughput tests, given that IPSec overhead in tunnel mode is around 50 bytes along with the new IP header, engineers found that the RenoGate delivered nearly 100% of theoretical maximum IPSec VPN throughput (across two Fast Ethernet interfaces) for 1,400-byte frames using 3DES/SHA-1 and SEED/SHA-1. This impressive performance as a SOHO appliance was mainly due to the hard-wired 2-by-2 switching IPSec processing engine embedded in FSC2003 SoC. Considering that the Future Systems' RenoGate is a residential gateway for SOHO networks, the test results showed that RenoGate equipped with FSC2003 SoC would hardly be a point of the performance bottleneck even with processing-intensive applications running.

In firewall throughput tests, the results showed that RenoGate in "bridge mode" processed 100% of the theoretical maximum throughput (acceptable loss rate ($\leq$ 0.001%) up to 500 firewall rules tested for all sizes of frames. In addition, the test showed that the firewall throughput was not degraded by the number of sessions up to 100 sessions tested.

In "router mode" test, except for the 1,518-byte frame size test, the throughput was the same as the one in "bridge mode" for all the test cases. The throughput from the 1,518-byte frame size test showed a very small amount of degradation by recording 198.8 Mbps when tested with 1 r/100 s, 500 r/10 s and 500 r/100 s (r: rules, s: sessions)

Test Configuration And Methodology

The Tolly Group/TTA tested the FSC2003 SoC (System on Chip) using RenoGate where FSC2003 SoC was designed for enhancing the performance of packet filtering and data encryption/decryption. The RenoGate can be configured as a firewall supporting various firewall rules and operation modes, or an IPSec VPN endpoint supporting typical encryption and authentication methods such as 3DES/SHA-1 and SEED/SHA-1.

For the firewall throughput test, engineers separately configured the RenoGate to operate in Layer 2 (Bridge) or Layer 3 (Router) mode with a single and 500 firewall rules, and with 10 and 100 UDP sessions. In this test, two Fast Ethernet interfaces of the DUT were configured in a full-duplex mode, with auto-negotiation enabled. Then, they were connected to the SmartBits 600 tester equipped with LAN-3301A modules and SmartFlow 4.50 test software.

Future Systems, Inc.

RenoGate with FSC2003 SoC

FSC2003 SoC Firewall & VPN Performance Evaluation using RenoGate

Future Systems, Inc.
RenoGate with FSC2003 SoC
Product Specifications*

RenoGate Specifications

Performance features

- Up to 200 Mbps firewall throughput (bi-directional)
- 200 Mbps SEED-SHA-1/3DES-SHA-1 VPN throughput (bi-directional)
- 10,000 concurrent sessions/20 concurrent VPN tunnels

Functional features

- Stateful inspection firewall
  - Transparent mode/Router mode/NAT support
- IPSec VPN
  - NAT traversal support
  - Certificate, preshared key-based IKE support
  - Split tunneling/Dead peer detection
- Active-Active high availability load balancing/fail over support
  - Kernel level VPN/Firewall load balancing/fail over support
  - Load balancing with external Layer2/Layer3/Layer4 switch support
  - Multi-WAN VPN load balancing
- Network attack detection and prevention (Scanning, DDoS, etc.)
- Static/dynamic routing support
- Management
  - Central and individual management/remote management support
  - Configuration backup/roll back support
  - Log-based real-time monitoring

FSC2003 Specifications

- RISC-type CPU
- Internal DMA / Quad 10/100 MAC
- Internal memory controller (Max. 128 MB)
- Two USB 1.1 host controllers
- Display controller
- Embedded 2-by-2 Switching Packet Processing Engine
  - IP/Non-IP packet filtering (Stateful inspection)
  - NAT
  - Statistics information of packets
- Embedded 2-by-2 Switching IPSec Processing Engine
  - AH, ESP, ESP with MAC, NAT traversal support
  - 3DES, AES, DES, SEED, MD5, SHA-1, HAS160 support

For more information contact:

Future Systems, Inc.
2F, 12F, Ace HighEnd Tower 235-2 Guro-dong Guro-gu, Seoul, 152-711, Korea
Phone: 82-2-6220-7732, Fax: 82-2-6220-7700
URL: http://www.future.co.kr

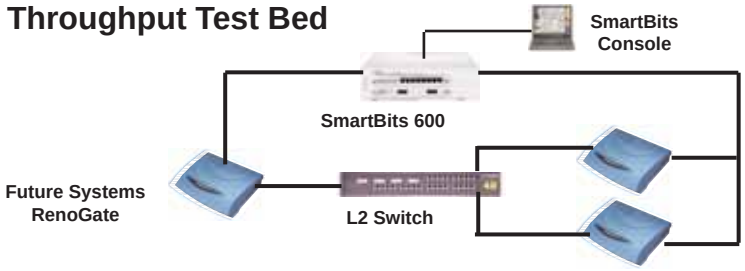
Vendor-supplied information not verified by TTA /The Tolly Group

The SmartBits generated bi-directional test traffic and measured the maximum steady-state zero-loss (≤ 0.001 %) throughput of the RenoGate for different frame sizes and for different test configurations. The test was repeated three times for each test environment - operation mode, the number of firewall rules and UDP sessions. The throughput test was iterated for each of frame sizes of 64, 128, 256, 512, 1024, 1400, and 1518 bytes and was run for 60 seconds.Two interfaces of RenoGate received and transmitted the test traffic simultaneously from the SmartBits where one was used to simulate a public side and the other, a protected private side.

When a single firewall rule was activated, all traffic was allowed to cross over firewall without dropping any packets. 500 firewall rules consist of 499 rules that deny the traffic matched up to the specified IP addresses, protocol and service ports. Then engineers verified firewall rules activated on the RenoGate by sending sample test traffic. The sample test traffic consisted of accepted stream and denied stream. The engineers sent the both streams to the DUT and captured the passed frames. Engineers verified that the firewall module operated properly and all the rules were active by analyzing the captured frames.

For the VPN throughput test, engineers used three RenoGates to create a two-tunnel configuration. (See Figure 4.) Engineers sent some learning traffic to establish and to verify the VPN tunnels before the production test. Engineers verified the establishment of tunnels by sniffing into the IPSec tunnels using a packet analyzer. Engineers measured the bi-directional VPN throughput by sending a single stream of UDP traffic from each direction for both tunnels using two different types of encryption and authentication methods.

VPN Throughput Test Bed



Source: TTA/The Tolly Group, December2005 *Figure 4*

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

Vendor	Product	Web address
Spirent Communications	SmartBits-600, SmartFlow 4.5	*http://www.spirentcom.com*
Agilent Technology	Agilent Advisor	*http://www.agilent.com*

Terms of Usage

USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability.

This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur.

The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers.

The Tolly Group provides a fee-based service to assist users in understanding the applicability of a given test scenario to their specific needs. Contact us for information.

When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.

Project Profile

Sponsor: Future Systems, Inc.
Document number: 205147
Product class: SOHO Firewall and VPN Applicance
Products under test: RenoGate equipped with FSC2003 SoC
Testing window: 25, October through 26, October 2005

Software versions tested: RenoGate v3.0.1.6
Software status: Generally available

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 sales@tolly.com, call (561) 391-5610.

The Tolly Group doc. 205147 rev. leechs 21 Dec 05