

## Stealth Networks – **Competitive Performance Test**

Stealth Secure Platform (installed on a SRVPN-10 device) Vs. Cisco 831-K9 small branch office VPN router

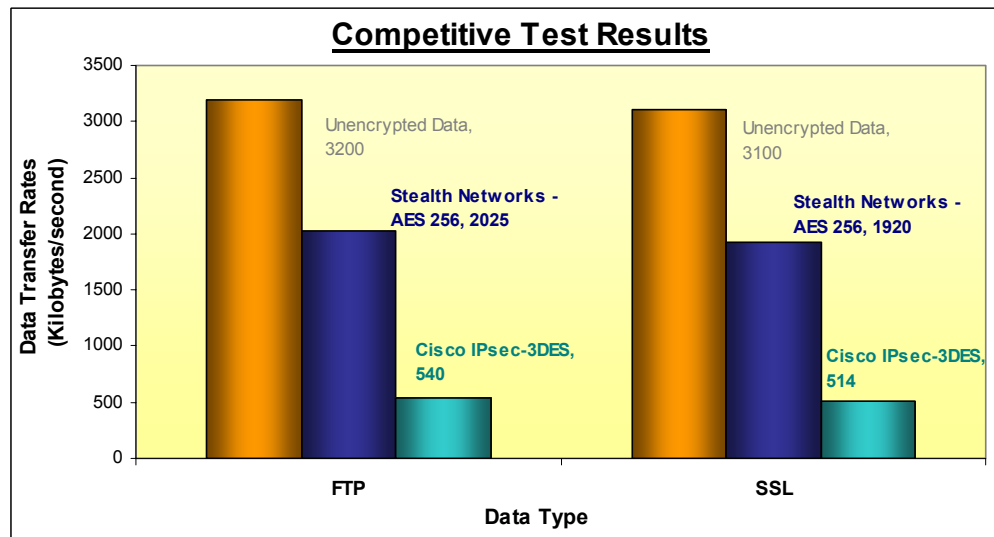
### Summary

agileTCP, Inc. was commissioned by Stealth Networks to independently verify that the Stealth Secure Platform provides 3-4X throughput compared to current market leading VPN solutions while providing higher data encryption (AES 256 instead of 3DES).

We decided to benchmark the Stealth Secure VPN router (SRVPN-10) that supports up to 10 LAN-to-LAN VPN tunnels with a Cisco router that has a comparable / superior feature set and price range. We finalized on the Cisco 831-K9 as it best matched the Stealth Networks router’s VPN, Firewall features while possessing additional hardware VPN encryption capabilities.

The tests proved that the Stealth Secure Platform delivered approx. 3.5 X more data throughput for both ‘plain-text’ as well as ‘SSL encrypted’ data traffic.

The SRVPN-10 also provided AES 256 encryption while the Cisco 831-K9 provided a lower (3DES) encryption. (See test setup and results below for details).



Overall, our tests show that the Stealth Secure Platform increases network performance in terms of bandwidth utilization and data throughput compared to current market leading VPN routers.

### Test Methodology

#### Objective

To measure plain-text and SSL encrypted data throughput across LAN-to-LAN VPN tunnels created with

- a. Two Stealth Network VPN routers (SRVPN-10)
- b. Two Cisco VPN routers 831-K9s

AND to compare the two data transfer rates.

#### Process Steps

- a. Connect the test hardware as shown in the network diagram (refer fig.1 shown on next page)
- b. Setup LAN-to-LAN VPN tunnels between the two SRVP-10s and the two Cisco 831-K9s

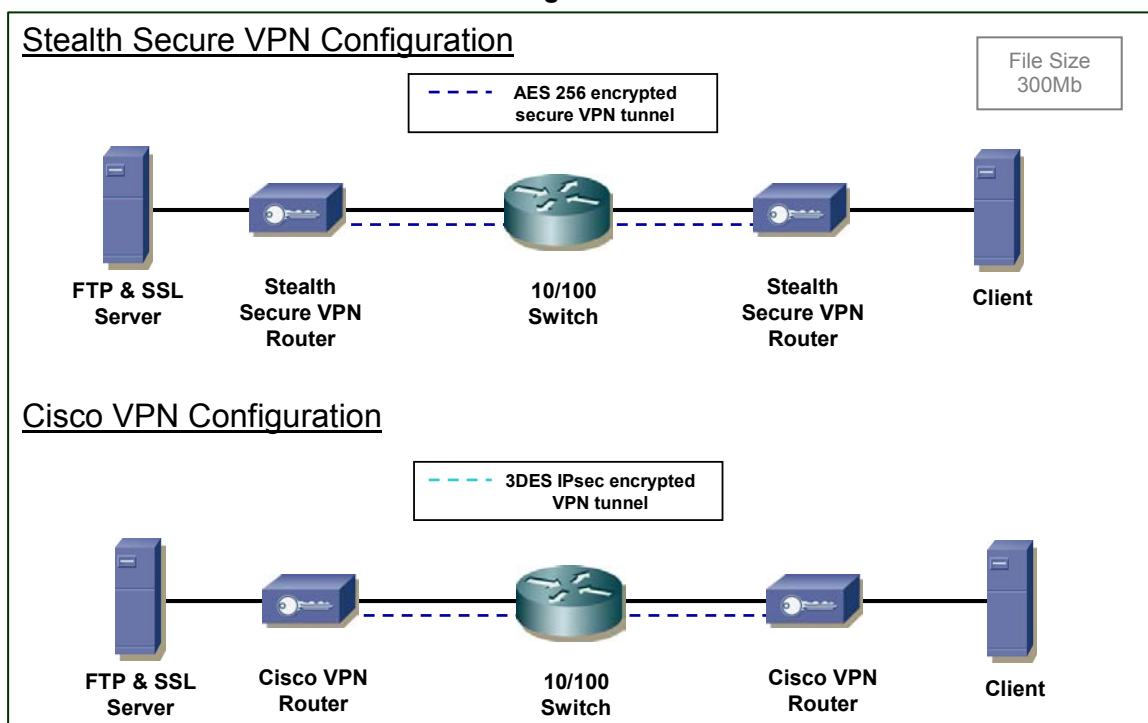
- c. Create stable data sources on both sides with a FTP and Secure Socket Layer (SSL) server on one end
- d. Create a 300 Mb (Megabyte) data file to simulate random Internet traffic
- e. Download the data file from the server to the client side machine through the VPN tunnels
- f. Use standardized tools (FTP and Windows file transfer) to measure data transfer rates in each case
  1. FTP – plain text & SSL encrypted data transfer with no VPN tunnels
  2. FTP – plain text & SSL encrypted data transfer through the Cisco VPN tunnels
  3. FTP – plain text & SSL encrypted data transfer through the Stealth Networks VPN tunnels
- g. Report measurements in a clear concise format

### Evaluated Technologies

- a. Stealth Secure VPN platform with AES 256 encryption
- b. Cisco VPN platform with 3DES IPsec encryption

### Network Diagram

**Figure 1**



Note - For the unencrypted data transfer – same network setup was used with no VPN routers connected.

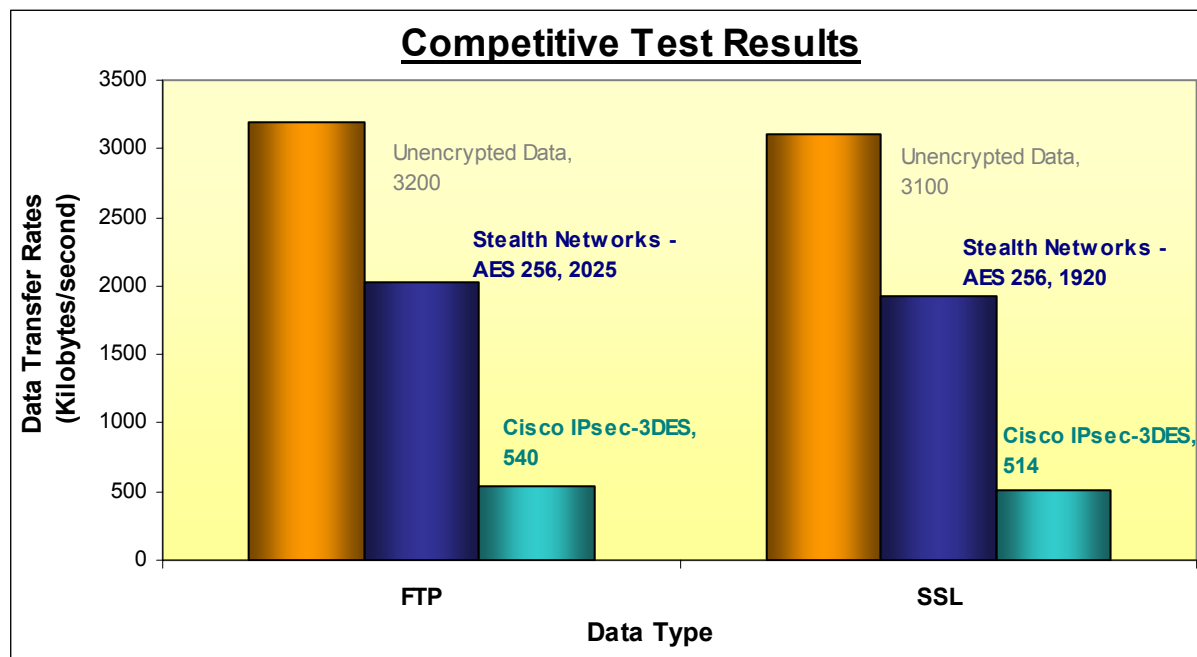
### Test Results

	FTP Xfr rate Kb/sec	SSL Xfr rate Kb/sec
Unencrypted Data	3200	3100
Stealth Networks - AES 256	2025	1920
Cisco IPsec-3DES	540	514

	FTP	SSL	
Stealth Networks / Cisco Throughput	3.75	3.74	= 3 - 4 X greater

### Actual Bandwidth Reserved for data

	FTP	SSL	
Cisco 3DES encryption	17%	17%	
Stealth AES 256 encryption	63%	62%	= 3 - 4 X greater



The Stealth Secure Platform provides better data throughputs and faster data transfer times for both plain-text and SSL encrypted data traffic. Typically data transfer rates are 3.75 X faster than the Cisco VPN routers.

### **Comments, Analysis & Conclusion**

- The Stealth Secure Platform provides network level security and hence is application agnostic. The platform performs better whether the application sends plain-text or SSL encrypted data in ASCII or binary mode.
- The data sources (client and server), the cables and the intermediate switch were kept constant throughout the test.
- The 300 Mb data file was created to simulate real Internet traffic instead of a straight binary file consisting of mostly zeros.
- The Stealth Secure software platform was loaded on OSI compatible PC hardware. Hardware can be scaled to meet additional user / tunnel requirements up to 64,000 simultaneous users on one server.
- The Stealth router hardware was comparable to the Cisco 831-K9 hardware in performance and price. Additionally, the Stealth Secure VPN routers did not have a hardware encryption chip while the Cisco routers did.

#### **Important Note –**

For the purpose of this test, the Cisco 831-K9s were configured with the basic firewall rules only while the Stealth Secure VPN routers had Advanced Firewall and IPS features enabled. Enabling similar features on the Cisco routers will presumably further increase their packet processing time resulting in slower data transfer rates.

The Stealth Secure Platform minimizes data packet overheads through the combination of alternate protocol use, open source IPsec encryption alternatives and data compression algorithms and hence maximizes bandwidth utilization and accelerates data transfers.

---

### **About agileTCP, Inc.**

agileTCP supports companies with information security compliance projects by applying domain expertise and project management skills in a principled manner. Typical projects include policy development, awareness training, technology implementation and event remediation. agileTCP is highly knowledgeable of industry specific standards (like SEMI 3509, E125...) and international standards (ISO 17799, BS7799...).

For more information, please visit us at [www.agiletcp.com](http://www.agiletcp.com)

#### **Disclaimer**

agileTCP has made reasonable efforts to ensure the accuracy and validity of this test. However, agileTCP specifically disclaims any warranty, expressed or implied resulting to the test results and analysis. All persons and entities relying on the results in this document do so at their own risk and agree that agileTCP, its employees, partners or sub-contractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing equipment, procedure or result.