Executive Summary
STOP Network Performance Testing

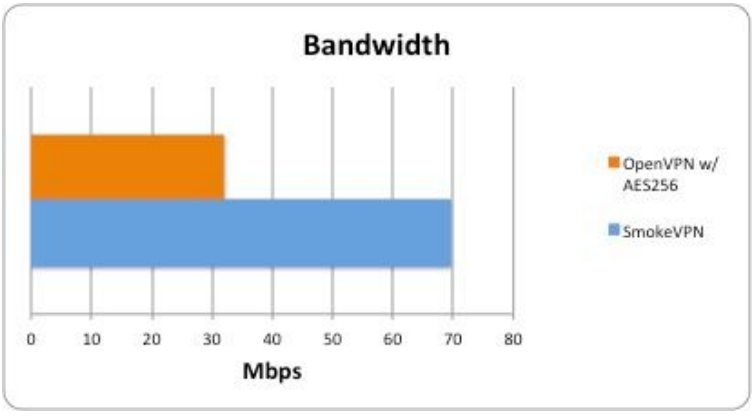
By: Dr. Nicole Nemer and Anthony S. Thompson
Editors: James Haid and Steven Cummings
Testing Conducted By: Dr. Nicole Nemer and Brian Mielke

Background and Methods

Introspective Networks has developed technology called STOP* that utilizes two main techniques to protect data: Moving Target Defense (MTD) - moving data in the network virtually and physically - and Streaming Key Encryption that utilizes a Vernam Cipher for data encryption. The solution utilizes two or more channels to separate and send both the ciphertext and streaming key at differing times separating them in both time and space.

STOP has been integrated into two well known technologies: a Virtual Private Network (SmokeVPN) and an IP Tunnel (SmokeTunnel). These were compared to one of the most widely used VPN/Tunneling solutions - OpenVPN with AES256 encryption. These comparison tests were conducted using three Processing Units (PUs), an *IN* SG4 gateway device and a VPN Web Service. Two sets of tests were run: 1) a LAN-based, PU to PU with a PU VPN server and 2) PU to VPN Web Service to SG4 gateway. Measurements were taken for CPU load, memory, network throughput and total data sent.

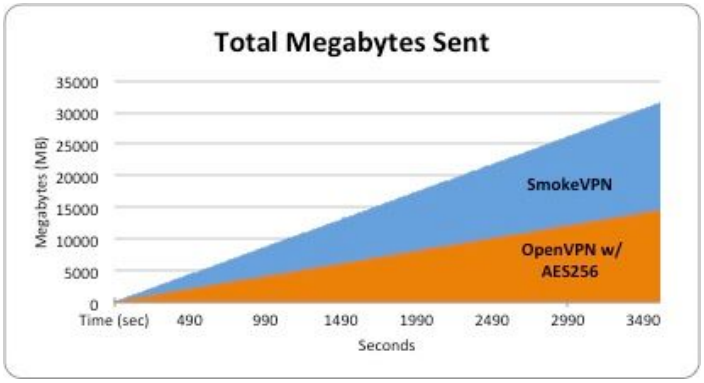
STOP resource requirements that are not needed by OpenVPN-AES256 include disk space and Key Stream processing. 8 GB of Streaming Key cache was used. These tests simulate extremely high PU load. In this scenario, Key Stream processing on the tested PUs would be load balanced to another PU in a cluster or offloaded to a Key Stream Generator. These tests simulate that condition.



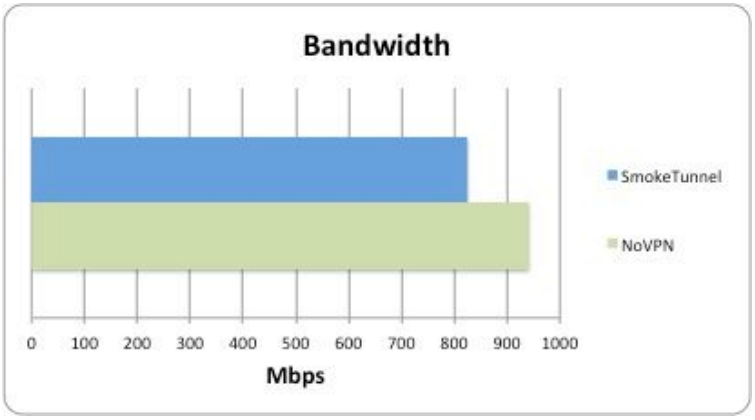
Results

The results were consistent when comparing SmokeVPN and OpenVPN. From the standpoint of network throughput on a LAN, SmokeVPN was over 2x faster and, as would be expected, delivered over twice as much data over the same period. Memory utilization for STOP was nearly 10 times higher but still under 35KB. In a modern computer system, this memory footprint is very small. CPU utilization for local network testing was also nearly 3 times higher for

SmokeVPN but, at maximum load, consumed less than one quarter of the CPU's total processing power. The resource utilization was due mainly to the overhead required for MTD security. Conversely, the network speed increase is due to the lower processing requirements of Streaming Key Encryption when compared to AES256. Over the Internet, where bandwidth was constrained, SmokeVPN still performed slightly better, coming in at 4mbps compared to 3.7mbps for OpenVPN. CPU utilization was closer with SmokeVPN using 4.21% of the CPU compared to 2.58% for OpenVPN. Memory was still roughly the same with the STOP solution at 29KB and OpenVPN at 3.6KB.



In our final test, we ran a STOP IP Tunnel - SmokeTunnel - against a scenario with no encryption at all. SmokeTunnel is a point to point tunnel with no server in between. The packet size was set to 64K which can only be accommodated in a local area network that is set up for packets that large. When testing in this configuration, SmokeTunnel ran at 82.5% of total bandwidth. The scenario with no encryption achieved 94.2%. SmokeTunnel CPU utilization was 29% while memory remained relatively small at 36.5K. This is a stunning result and shows that SmokeTunnel's bandwidth is only around 12% less than no encryption at all at GigE speeds.



In summary, STOP enabled VPN solutions outperform OpenVPN-AES256 in the critical area of network performance in every instance. With a STOP tunneling solution using 64K packets, performance was higher than 80% of full line rate. CPU, memory, disk and even network utilization to send the streaming key are all higher with STOP. With that said, the resources of today's modern compute systems keep these values within an acceptable range for most applications.

** STOP - Streaming Transmission One-time-pad Protocol*