

UTM and FIOS...Too Much Bandwidth to Inspect

PRINT

September 06, 2007

By Matt Brunk

Several months ago, I purchased a NFR (not for resale) firewall to install at home. I've worked with the product for a couple of years now and the idea behind the purchase was to enforce content filtering and set up limits for my 11 year old daughter.



Unified Threat Management (UTM) is a great tool and in spite of any firewall using resources for anti-virus/anti-spam enforcement, authentication, content filtering, intrusion and gateway protection, VPNs and reporting- they all use resources and the throughput isn't going to match what you get without a 'stateful' inspecting firewall.

The issue began when my wife pointed out that the Internet is now slow! "What did you do!" Note- it wasn't a question but instead a well deserved accusation. She's the primary user so she should know. I didn't know.

I removed the firewall and re-installed the free router from Verizon. My bandwidth returned to 5.4 Mbps down / 2.1 Mbps up using the **SpeakEasy Speed Test**. Next, I placed the firewall back on-line and removed the free router. Using the same test my bandwidth returned a 2.1 Mbps down / 1.86 Mbps up again using the same test. I adjusted the **MTU** from the default MTU size of 1500 and incrementally ran the scale in increments of 8 downward- with no improvement. After calling Verizon, we even tried using the **TCP/IP optimizer** found on the Speed Guide website to no avail. Then, I tired some other tricks but all were in vain. I called the firewall Tech Support at different times and got different answers and suggestions but not an explanation until I fired off an email. I explained "at a customer site we tested the same firewall model with the same OS, and implemented features and licenses. The difference in the firewalls- the customer site is using authentication and at home, we're not. Their ISP is a dedicated T1 (1.544 Mbps) and their results were 1.39 MBps down / 1.4 Mbps up. "

So I know my wife is right- I'm losing over 50% of throughput because of the firewall, I installed. Why not just put back the old firewall?

According to the firewall manufacturer- "Our R&D team is looking at addressing this in a number of ways, but to reiterate, this is not a competitive disadvantage for brand-X. Any other vendor who is scanning every packet for full UTM services is in the same boat as we are. It's not an ideal answer, but I do want to make sure you're aware that we're not at a competitive disadvantage with this; the entire security market (in particularly UTM vendors) is working on addressing this right now."

So to keep peace in my family- I've exempted my wife's PC from content filtering- so she won't get the message "Please see Mommy or Daddy about the website you are attempting to visit." It doesn't solve the real problem of not having enough speed or throughput. A firewall that isn't stateful inspecting such as the FREE one supplied by Verizon does allow throughput with much less loss. What worries me is what else does the FREE firewall allow that we don't want. It's an old lesson from the military- which do you want first: speed, security or safety? You don't get all three without compromise.

This is important to note that Verizon FIOS is making headway with a long stretch into homes and multi-unit dwellings including businesses. More bandwidth means plenty of opportunity for the bad buys. The stateful firewall touching FIOS must be capable of inspecting lots of bandwidth. The trade-off of using a non-stateful firewall or simple NAT is security. The UTM appliance does more at the cost of bandwidth. The limitation I ran into impacts everything from voice to user demands. What I don't appreciate hearing is "upgrade to the next model which is indeed a much more capable product built to serve M-enterprise. That isn't a practical solution for a budget minded wife that expects to have Internet the way it was before I started playing Daddy IT.

Comment on this Article

[Click here to comment... \(Show/Hide Form\)](#)

Other Visitors Comments

There are no comments currently....

Close Window