

David Laliberte

From: Mike Edenholm [medenholm@westtel.ky]
Sent: Wednesday, April 14, 2010 12:45 PM
To: David Laliberte
Subject: Corporate DPI
Attachments: dpi corporate final.doc

Hi David,

Here is the corporate document that we were going to send out to customers.

On a separate note, I noticed a lot of the submissions from the legal groups were all about privacy. Would it be helpful for WestTel to submit as part of a response the fact that dpi, no matter how good, cannot examine the contents of an encrypted packet? That would include https, vpn, and other pki transmissions.

There is also quite a bit of concern in various forms about advertising inserts and redirecting traffic. WestTel does not currently have the ability to either of those feats. Does it make any sense to discuss?

I keep thinking that this is like the government putting a ban on automobiles because they have the possibility of exceeding the speed limit.

Anyway, I think in both documents we met the points laid out in the decision.

Thanks,

Michael Edenholm

Chief Executive Officer
WestTel Limited

✉ edenholm@westtel.ky
☎ +1 345 745 2739 (Main)
☎ +1 345 743 0001 (Direct)
☎ +1 345 938 0001 (Cell)
☎ +1 345 743 0604 (Fax)
www.westtel.ky

E-MAIL CONFIDENTIALITY NOTICE: This e-mail, including attachments, is confidential and may contain information that is privileged, proprietary and non-public. It is intended solely for the addressee(s). Access by any other person to this e-mail is not authorised. Any unauthorised disclosure, copying or other distribution of this e-mail, including attachments, is strictly prohibited. If you have received this e-mail in error, please notify the sender immediately and delete the e-mail without reading, copying or forwarding it to anyone.

Dear Corporate Customer

We have been instructed by the ICTA to update all of our Corporate customers regarding our use of Deep Packet Inspection (DPI) technology. This letter seeks to provide an overview of WestTel's use of this capability.

By default, WestTel does not utilize DPI technologies to manage traffic on corporate internet or point to point circuits.

However, WestTel can, if requested, create a traffic profile that can assist your business in better managing its communications assets. DPI technologies provide a powerful tool for accelerating, blocking or reducing the priority of network traffic based upon application. To date, a number of customers have requested and received this service from WestTel.

So if your business is experiencing sluggish network performance, WestTel may be able to help at a fraction of the costs normally associated with upgrading your bandwidth subscription. Should you have any questions regarding the information contained within this communication, please email us at 'business@westtel.ky' or call the business team at (345) 743 4343.

For more information on the public consultation concerning DPI technologies, please consult the following link.

http://www.icta.ky/da_public.php#dpi

Regards

Michael Edenhalm
CEO, WestTel Ltd.

Within the Residential market, DPI technology is used, during peak traffic periods only, to ensure the best possible internet experience for all customers. The technology allows WestTel to determine the specific application types running across our Residential platform at any given time. During peak traffic periods, time sensitive applications, such as VoIP and Video are given priority over connectionless applications such as Peer to Peer, FTP and email. Within this scenario, our sole intention in the use of DPI is to ensure the very best experience possible for all of our Residential customer base.

Internet security is of prime concern to WestTel. Our network operations team utilize a number of tools in order to manage SPAM, viruses, phishing, and denial of service attacks. DPI technologies provide network operations with the ability to identify and block threats both external and internal to the WestTel network.

We should also highlight the fact that our use of DPI is purely for real time 'dynamic' management. We do not, at any time, store any of the data associated with our interrogation of the network, nor do we redirect, insert or in any way alter the data transmitted on the network.