



SECURITY IMPLICATIONS OF MOVING FROM HUB-AND-SPOKE TO MPLS

MPLS delivers many benefits, including reduced congestion due to added flow path control, easier creation of VPN tunnels, Quality of Service and reduced network complexity. However, Enterprises are finding many network security repercussions from migrating to MPLS networks.



Figure 1

Traffic Flow on a Hub-and-Spoke Network

Prior to MPLS, a cost-effective Intrusion Detection System (IDS) deployment may have required security devices at the hubs only of a hub-and-spoke network. In order for traffic to travel from the Seattle, WA facility to the Denver, CO facility, it first must pass through the Atlanta, GA Data Center, as depicted by the orange arrows in Figure 1. With this network model, the IDS in the Atlanta Data Center inspects all traffic passing between facilities. It is important to realize, however, this security "visibility" can only be maintained as long as traffic reliably passes through the hub.

Traffic Flow on an MPLS Network

MPLS introduces the potential for the "spokes" to communicate directly with one another, bypassing the "hubs" and security devices resident within. As depicted by the orange arrow in Figure 2, traffic can now travel from the Seattle, WA facility to the Denver, CO facility without first going through the Atlanta hub. Consequently, all facilities can communicate with and infect one another without the protection of an IDS at the hub, thereby eliminating visibility into this "inter-facility" network traffic.



Figure 2

Is There a Cost-Effective Solution?

Enterprises considering MPLS migrations should evaluate a more cost-effective and complementary method of monitoring traffic that transits the MPLS cloud. By choosing a NetFlow™ or sFlow® StealthWatch solution instead of deploying IDS sensors at each MPLS-enabled site, Lancope customers saved both upfront expenses and ongoing administrative costs associated with deploying, tuning and upgrading scores of extra IDS sensors. In addition, StealthWatch enabled them to:

- regain network visibility into all host behaviors and all network traffic during and after the move to MPLS with a centralized deployment of StealthWatch
- increase confidence in security personnel workflow prioritization to immediately identify compromised hosts and dramatically limit the impact of network incidents
- monitor the network, identifying incidents that may affect network and application availability

How StealthWatch Works

At each MPLS-enabled WAN location, NetFlow or sFlow technology is enabled at the remote locations' router(s). Detailed information about the traffic flowing from site to site is transmitted across the MPLS cloud to a central StealthWatch flow collector appliance. As the flows arrive at the centralized collector, StealthWatch performs behavior analysis to reveal network congestion issues, policy violations, worm outbreaks and other security-related incidents.

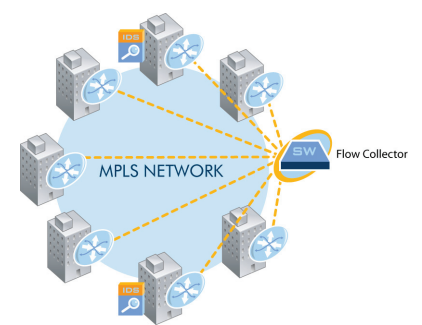


Figure 3

For more information, please contact 888.419.1462 (US), +1 770.225.6500 (International), or sales@lancope.com