ONPATH TECHNOLOGIES
ALWAYS ON

White Paper

LAWFUL INTERCEPT AND CYBER SECURITY:

DELIVERING CRITICAL INFORMATION WHEN AND WHERE IT IS NEEDED

By: O.J. Johnston, ONPATH Technologies

A few decades ago, Lawful Intercept (LI) was a relatively simple concept. If a person of interest was targeted by a Law Enforcement Agency (LEA), the LEA could get a warrant to "tap" the person's phone. Once the warrant was issued, the LEA could contact the local phone company to tap the phone line allowing the LEA to listen to the target's conversations in real-time for the purpose of gathering incriminating evidence.

Over the last two decades, LI has become a much more complex issue. Now, people worldwide communicate over the Internet via email or Voice over IP (VoIP). As our communication has gone from an unencrypted, circuit-based infrastructure to a highly encrypted, high-bandwidth, packet-based infrastructure, the challenges with accessing incriminating evidence in real time are anything but trivial. Not only are peoples' conversations interspersed with one another across the Internet, but many times the conversations are encrypted to protect privacy. Furthermore, due to the explosive growth in Internet traffic, as shown in Table 1, techniques have been developed to maximize bandwidth and prolong the life of network protocols by manipulating packet encapsulation and addressing information complicating the ability to isolate a single conversation.

In the traditional sense of LI, there are standards and rules associated with identifying Internet traffic for the purpose of pursuing a criminal investigation. However, there is another side to LI that is related to surveillance for intelligence gathering against both traditional and cyber terrorists. After the attacks of 9/11, the government realized that terrorist organizations were using the Internet to communicate, relying upon our laws to ensure their communications would not be intercepted or, if they were, it would likely be too late. To effectively fight the war on terror, our current and past Presidents changed the Foreign Intelligence Surveillance Act (FISA) to allow our Intelligence agencies to monitor traffic entering or leaving our country in real-time for the purpose of identifying terrorist activities including cyber attacks. While it has been suspected, and in some cases documented, that government intelligence agencies spy on each other, the 9/11 terrorists attacks forced governments to look at individuals operating on their own, or as part of a group, but not officially affiliated with any government. Today, any international conversation believed to be terrorism- or cyber security- related can be legally intercepted without a warrant.

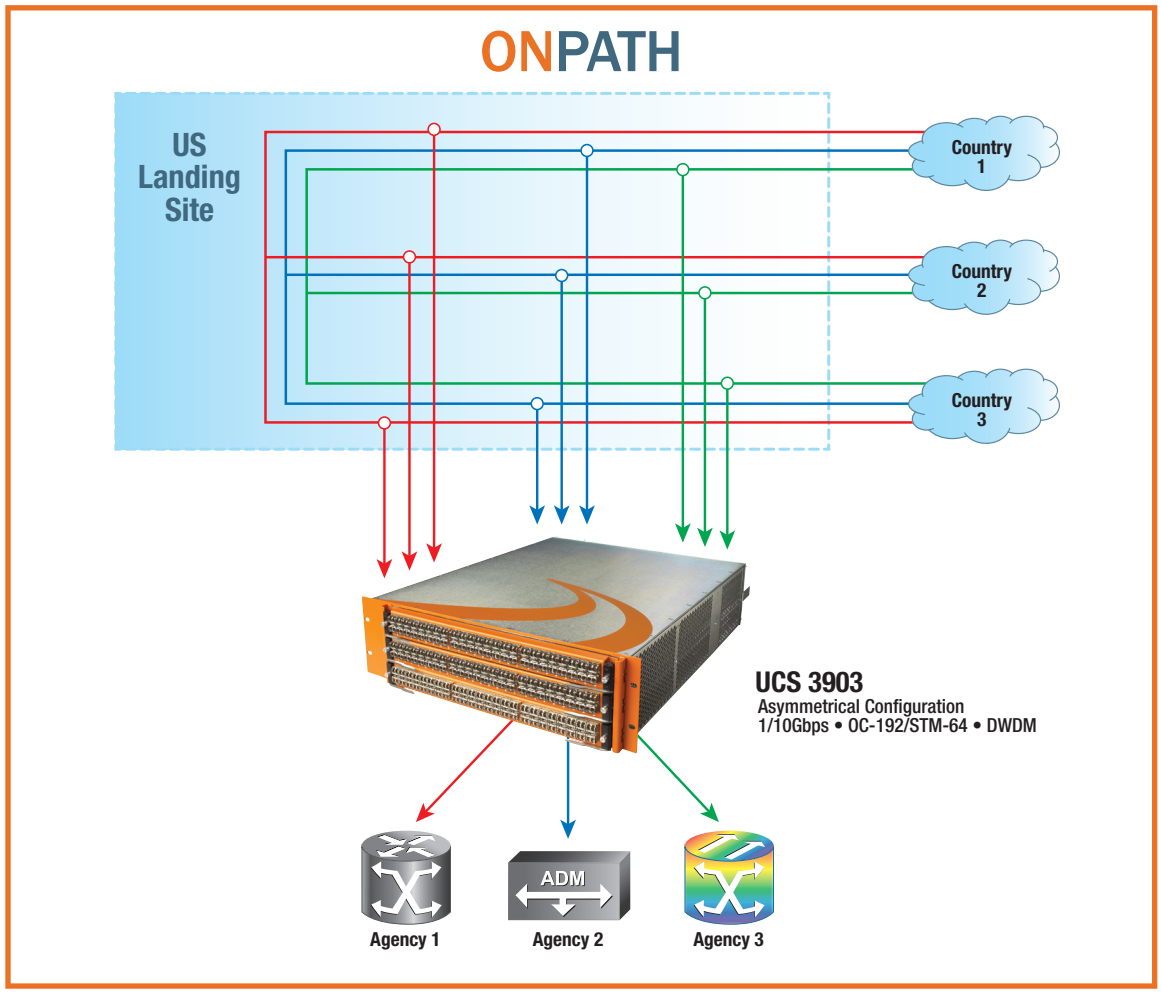

FIGURE 3 ONPATH-optimized solution for Lawful Intercept reduces the amount of required network equipment and dedicated circuits for each agency

CONCLUSION

With the changes in "warrantless" Lawful Intercept, new challenges have emerged in how information is collected and ultimately distributed to intelligence agencies. Carriers need efficient and cost-effective ways to pass traffic to the various agencies without impacting their networks. Likewise, agencies need optimized resource utilization to access information of interest on any carrier's international network. In addition, agencies need to be able to efficiently share information without compromising security. ONPATH Technologies offers solutions that enable agencies to deliver critical information via secure, non-disruptive tapping, when and where it is needed, without compromising cyber security. Ultimately, ONPATH enables Cyber Security applications to implement the critical security measures required while helping conserve time, increase network utilization, and save money.

ONPATH TECHNOLOGIES

ABOUT ONPATH TECHNOLOGIES

ONPATH Technologies is the leading provider of scalable connectivity and monitoring solutions for high-performance networks. With a history spanning over 25 years, ONPATH is a spin-out of Brocade Communications' physical layer switch business. ONPATH's Universal Connectivity System™ and HorizON™ Software deliver an advanced platform that automates and secures data center and test infrastructure to help network managers conserve time, increase utilization, and save money compared to manual patching or complex mesh switching architectures. Our patented switching technology and advanced software deliver the industry's most scalable, secure connectivity solution with the most in-depth view of your network. Scalable from 8 to 4,096 non-meshed ports, independent of your speed or protocol requirements, ONPATH delivers the flexibility and security required by today's data centers and the investment protection necessary for those of tomorrow. ONPATH currently has over one million installed ports throughout Fortune 1,000 and Government customers.

For more information on how ONPATH can help you with your initiatives, contact us today for an engineering application review or network consultation.

2000 Lincoln Drive East
Marlton, NJ 08053
609.518.4100
info.request@onpathtech.com
www.onpathtech.com