Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 12, Issue 5

SDN-driven telco networks call for pervasive network visibility

By Andy Huckridge

It's no secret that the telecommunications market is in the midst of a significant transformation. The number of mobile devices and users has skyrocketed in recent years; according to research by GSMA, there were 3.6 billion unique mobile subscribers at the end of 2014. Half of the world's population now has a mobile subscription—up from just one in five just 10 years ago—and an additional one billion subscribers are predicted by 2020, taking the global penetration rate to approximately 60%. Further, projections for IoT devices that will need to communicate using these same networks are astronomical. Gartner, Inc. forecasts that 4.9 billion connected things will be in use in 2015, up 30 percent from 2014, and will reach 25 billion by 2020.

With more users and devices comes an explosion of data being delivered to them, which has increased network complexity. According to Cisco's Visual Network Index, global mobile data traffic reached 2.5 exabytes per month at the end of 2014, up from 1.5 exabytes per month at the end of 2013. This is a growth of 67% in just one year. Operators are struggling to ensure their networks are flexible, scalable and secure enough to support these escalating data demands, while at the same time ensuring they continue to offer high levels of service. In a market that already sees high levels of churn, operators have to keep Quality of Service (QoS) high to hold onto their customers, as well as introduce new services to differentiate themselves. In order to do this, as well as deal with continuously increasing traffic, a transformation is required.

100G networks aimed to solve the issue of too much traffic, but are hard to monitor as associated analytic tools are unable to directly connect, while mobile services like VoLTE are complex and very sensitive to real-time performance, requiring a high level of visibility to keep them functioning. On top of that, virtualization technologies, such as software-defined networking (SDN) and network functions virtualization (NFV) – are becoming increasingly attractive propositions, thanks to their promise of simplicity and agility. Yet they also add layers of network abstraction, which decreases visibility into traffic crossing the physical layer. Essentially, a telecommunications network is a very complex environment, and the challenges don't stop there.

Overcoming the network security challenge

Like other industries, security threats to carrier networks and services are increasing every day and the tactics used by adversaries are sophisticated and wide-ranging. SMS fraud, malware, DDoS attacks, and data ex-filtration are just some of the ways cyber-criminals can compromise a mobile network. A cyber-criminal only needs to find one vulnerability to exploit, while the network operator needs to protect the entire infrastructure. And while these threats to carriers are growing, security infrastructure is becoming more complex and costly to manage and operate.

The introduction of SDN to service provider networks increases network vulnerabilities. For example, separating the data and control plane in an SDN deployment that could lead to synchronization issues between these two components. Also, when virtualizing a network using encapsulation or tunneling, organizations must create separate logical overlays which are abstracted from the physical underlying network, creating two planes of troubleshooting, monitoring, and management—the physical underlay and the logical overlay. Both planes can be subject to security threats and breaches.

To work around this, real-time visibility into the entire network environment is required so threats can be identified and removed as quickly and as seamlessly as possible.

You can't secure what you can't see

Today, service providers still battle with "stovepipes" design, where pervasive network visibility is defeated. One group inside the organization is unable to share visibility with another group. Also, SPAN and Mirror

ports drop packets routinely, so insight from the traffic can be lost when the network is under load—the most important time to understand what is happening to the traffic on the network.

Without the required visibility, packets will be dropped and blind spots will occur, making it easier for nefarious actors to access and remain on service provider networks. Operators need to conduct real-time analysis of data streams in order to detect and prevent criminal activity as quickly as possible. To do this effectively, they need pervasive visibility into network traffic. Real-time analysis of packets is also required; yet with the sheer amount of data that they need to sort through, this can be a challenge. These visibility tools require a security delivery platform that will intelligently feed the tool with the specific data packets and streams they need – and nothing else. They also need GTP tunneling.

GTP Tunneling

GPRS Tunneling Protocol (GTP) is often used to carry mobile data across networks, and includes control plane and user data plane traffic. Currently, many analytic and security tool vendors have a built-in feature to correlate GTP, the user plane, with the control plane inside GPRS tunnels. But in the process, each analytic tool hides its insight from the other analytic tools—and it's this subscriber and service layer insight that is needed. As such, the operational efficiency of the service provider decreases thanks to the increased cost of reduced tool processing throughput—which also reduces the effectiveness of security tools.

Visibility into subscriber activity requires the ability to understand the stateful nature of GTP traffic and correlate subscriber-specific sessions in order to gain an accurate view of the subscriber's activities. Once this is achieved, the traffic can be intelligently sorted to optimize flows based on what the tools need to see, so the applications used to secure, monitor, and analyze the infrastructure see only what is relevant to them.

From there, tools designed specifically to identify suspicious activity can do their job—without having to sift through petabytes of irrelevant data—so that they can quickly stop criminals in their tracks.

Whitelists

Another tactic for ensuring network security involves the creation of a whitelist. Mobile carriers can create custom whitelists of specific subscribers using their IMSI (International Mobile Subscriber Identity).

For example, if a service provider needs to identify security threats from an individual subscriber or device, they need to focus on specific subscribers or devices that present a security threat to the network. They also need to remove malicious traffic from the network, or deny it access to the network. Since security tools rarely run at line-rate speeds, any capability that reduces the amount of traffic flowing through the tools provides for a smaller and more cost-effective security capability, giving the operator the ability to do more with less.

As threats increase and become more sophisticated, and as network architectures change with SDN and virtualization, the need for visibility increases - particularly in large carrier networks.

Whitelists can be created to identify security threats to (or from) a specific subscriber. This results in a clear operational advantage by reducing operational costs and freeing up network capacity. Meanwhile, subscriber devices and associated malicious traffic can be blocked from the network altogether.

Whitelisting and GTP correlation can also be used to treat devices, applications or subscriber groups with a perceived higher security threat profile—such as a specific vendor and their associated devices and apps that may be lacking built-in security screening capabilities—differently. This way, traffic can be grouped with low-threat traffic being treated differently than high-threat traffic. This preserves the processing throughput of security tools, decreasing the cost for processed traffic, which yields a competitive advantage against other competing carriers within a region.

Pervasive network visibility is critical

As threats increase and become more sophisticated, and as network architectures change with SDN and virtualization, the need for visibility increases—particularly in large carrier networks.

As SDN becomes more pervasive, the need for traffic-based visibility solutions in such an environment, along with increased correlation of traffic with controller policies and state, will need to become an integral part of the SDN solution. Further, the dynamic nature of the network, compute and storage, will drive the need for delivering traffic pervasively across all segments of the

network to a centralized set of tools responsible for the monitoring and correlation of performance, security analysis, and user experience.

This calls for a new approach to securing the network all together—one that shifts from perimeter-centric prevention to a model more focused on detecting breaches by providing consistent access to relevant data from physical and virtualized systems. Such a model will dramatically shorten the timeframe between breach and detection, helping operators to ensure consistent, secure service to their customers.