# Why Deep Packet Inspection is Vital to Functioning Securely in the Cloud

While the cloud is often thought of as an ethereal space, it is in reality a physical place where data is stored. And wherever data resides, hackers will attempt to compromise it. Ultimately, hackers want to get into a company's network and the cloud can be an effective conduit to achieving that objective.

Providers are responsible for protecting the data within their cloud, but vulnerabilities are inevitable, and in the end, network security rests in the hands of the enterprise. This means being able to visualize everything coming in and going out of the network. The egress point from the network and the ingress point for accessing cloud data are the two major areas where attacks can occur, as well as where they can be detected.

Gaining visibility into these two points is crucial to achieving much needed security within the cloud. Deep Packet Inspection (DPI) is the best way to attain this visibility. DPI offers the ability to alert enterprises about aberrant behavior, unusual IP addresses, ex-filtration attempts and other methods of attack. DPI makes it possible to block many attack methods, while assuring that data and the network are not compromised.

## With Growing Cloud Adoption Comes Security Concerns

Migration to the cloud continues unabated. In many cases, enterprises are utilizing more than one cloud provider to meet their robust business needs. A recent survey found that more than 50% of respondents reported using between two and six public cloud providers. Because each provider sets its own security and configuration rules for servers, apps and containers, managing risk across all cloud implementation becomes a significant challenge.

This security management problem is made all the more difficult when IT skill shortages are factored in. A cloud security survey reported that 28% of respondents cited insufficient skills or training around specific public cloud services as their greatest concern when dealing with cloud environments.

## DPI Delivers Much Needed Cloud Visibility

Many cloud services are accessible to the entire Internet, and, after all, an important driver for cloud migrations is the improved accessibility of systems. This means cloud servers and applications are exposed to potential attacks by a broad range of methods from anywhere around the globe. This is where Deep Packet Inspection (DPI) can make a difference. There are many threats to using the cloud, and just like in an enterprise's private network, IT must monitor and use DPI to visualize the data and aberrant behavior. DPI should be the first line of defense in protecting data integrity and security processes. Put another way, DPI delivers the visibility and insights needed to keep the bad traffic out, while letting the good traffic through without too much interruption.

Taking this a step further, security measures need to look past the perimeter-based defense layer, focusing more inwards. Lateral movement between a compromised (cloud) system and other systems, both within the cloud or on-premises, can be particularly difficult to detect. DPI has proven its ability to deliver visibility into these lateral movements between systems, including software-as-a-service (SaaS), the main cloud technology. Once armed with these critical insights, security teams can detect and potentially block incursions.

DPI can play a pivotal role in detecting invalid and malicious cloud activity indicative of data leaks and breaches, as well as access management incursions, by:

- Verifying and validating legal entries and methods of access
- Recognizing known attack vectors and methodologies
- Alerting to unusual records download both in type and numbers
- Recognize data traffic changes

**The Good, the Bad and the Ugly of DPI and the Cloud**

While DPI is clearly a powerful and effective tool for supporting the protection data in the cloud, there are several privacy concerns that are occasionally raised. The data in network packets can contain sensitive information, including social security numbers, credit cards details and even passwords. In a perfect world this data should be encrypted, but this is not always the case. And encryption is not always sufficient protection. In the case of SSL interception, cyberattackers intercept encrypted traffic, then decrypt it and analyze it for nefarious purposes.

Another security shortcoming is that cloud providers do not like to give their customers close access to network traffic within their multi-tenant platform. Without full access to DPI, it becomes more challenging to implement customer-to-customer data leak security protocols.

Finally, the network traffic within a shared cloud platform is effectively encapsulated in order to separate the customer and management flows, which often means traditional network-based DPI solutions will experience challenges processing the observed cloud traffic.

**Successfully Deploying a Security Control Based on DPI**

There are several approaches to successfully deploying a security control based on DPI within a public cloud environment. The first one is to use the vendor solutions already built for this exact purpose. These could be virtual instances, such as the Sophos UTM9 product, a next-gen firewall product with inbuilt IDS and Application Layer 7 controls (for which DPI is required). The benefit here is the ease of deployment, support and management.

Another product range is based on agents running on customer endpoints. The endpoints not only process network traffic, but also forward a copy of selected (or all) raw traffic to a security monitoring system. Metaflows offers such a product. The benefit here is that network encryption, such as SSL, is less of a challenge because the endpoint should see much of the data in unencrypted form.

Finally, a virtual network TAP, for example offered by AWS, can provide a full network traffic feed to any destination. This could be an intrusion detection system, a Netflow sensor, or a malware sandbox. Although the destination system is not directly inline, the extensive flexibility of this option allows for inter-device messaging where, for instance, an IDS automatically directs a firewall to block a malicious IP detected by an IDS signature.

### The Evolution of DPI: Deep Content Inspection

A modern evolution of DPI is Deep Content Inspection (DCI). Where DPI covers the analysis of data inside individual network packets, DCI is capable of detecting how multiple packets together can make up a file or data stream. This is usually done by the detection of a certain MIME (file) type, after which the data is captured, reconstructed, and analyzed by, for instance, an antivirus or malware sandbox application.

DCI has been adopted in most products that support DPI, and the terms are sometimes intermixed because they are quite similar. However, proper DCI offers some major advantages. For instance, it has made it much harder for an attacker to break up malicious code into smaller packets in order to bypass an IDS device. It also provides the ability to dynamically analyze entire (often encrypted) extracted malware files, making it possible to observe suspicious behavior. The solutions mentioned here around DPI usage within a cloud environment are mostly applicable for DCI, as well. Some performance overhead can be expected, because of the sessions that remain open while files and data streams are reassembled.

The bottom line is - data is valuable! It must be protected, and any attempt by cyberattackers to compromise that data needs to be recognized. DPI and DCI are the latest technologies to protect and verify an enterprise’s data.