NETSCOUT

| WHITE PAPER |

Understanding and Engineering Network Traffic

With OTT and Service-Layer Visibility

SECURITY

TABLE OF CONTENTS

In the past, traffic analysis and engineering based on criteria such as IP address allocation or ASN was sufficient. For example: traffic from home users to Google, or governments, or banks was clearly seen and reliably understood, since those services were discrete and provided in-house by those organizations. Network engineers and operators were able to easily understand their traffic loads and routing, and engineer their environments accordingly.

As the Internet has grown, simple IP connectivity became difficult to categorize if it didn't involve a very specific, known type of customer or business. As cloud, service, and hosting provider usage became more mainstream, the veracity of IP address or ASN identification as a means of reliable categorization of traffic has waned.

Today, CDN services and the ubiquity of large-scale cloud providers like Amazon and Microsoft make any useful categorization impossible when strictly looking at traditional criteria such as IP addressing or ASN. Today a single company might serve millions of customers, spreading its offerings across multiple cloud providers regionally or even globally, and not even have a registered BGP ASN or IP block allocation – relying entirely on that level of connectivity from the cloud providers themselves. This renders IP and ASN identification useless when trying to understand the nature of the traffic itself.

The challenge has become determining what services are actually being utilized when IP addresses or ASNs are not providing enough insight. Therefore, we must begin to correlate additional resources with the IP connectivity to ascertain what is happening. Utilizing DNS provides a significant insight into the nature of a connection. By correlating IP connectivity with DNS requests, we can begin to more accurately and finely categorize this traffic as well as establish user intention.

Additionally, Over-the-Top (OTT) services (predominantly streaming video such as Netflix and HBO, which historically were delivered over cable and satellite mediums) have become mainstream, making identification and classification simultaneously more important and even more difficult.

Intelligent and economical network architectures and peering can make a large difference from the user experience all the way to ISP cost-savings. If traffic can be more intelligently categorized, companies can utilize this insight to better optimize their paths and links to content their users are consuming.

Arbor Sightline combines the technologies of NETSCOUT® and Arbor to deliver smarter traffic visibility, as well as an automated, fully integrated DDoS defense. Sightline delivers a unique combination of broad and deep visibility, building on the Arbor network visualization and leveraging NETSCOUT Smart Data. Arbor Sightline provides deep insight into the service-layer, delivering OTT traffic analysis across complex networks.

Today, network optimization is not just about the total volume of network traffic, it is about delivering desired content most efficiently while minimizing peering and transit costs. Sightline allows network operators to understand where and how major content services are traversing the network in order to optimize both user experience and peering and transit relationships.

T-Mobile's Neville Ray says that use of education apps like Google Classroom and Khan Academy has skyrocketed, growing 167% since the beginning of March. Use of collaboration tools like Slack, Webex, and Zoom has also exploded, as more people use them to stay in contact with colleagues and loved ones. Usage of those apps has grown 137% over the last month.

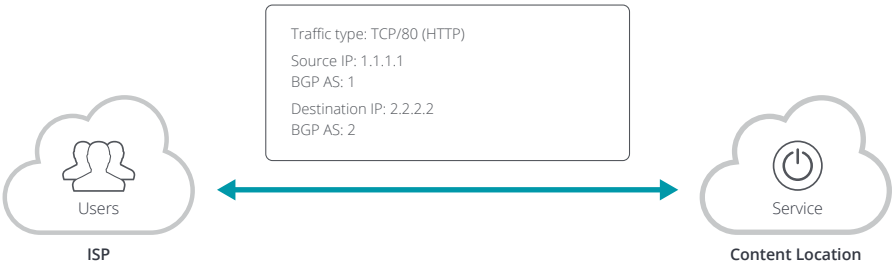
https://www.tmonews.com/2020/04/t-mobile-sprint-customers-network-usage-coronavirus-pandemic/

The new normal telecommuting may be a bit more permanent than realized, as 74% of CFOs say they expect to move previously on-site employees remote post-COVID-19, according to a Gartner survey.

https://www.zdnet.com/article/cfos-looking-to-make-remote-work-telecommuting-more-permanent-following-covid-19-says-gartner-survey/

What Does a Basic Connection Look Like?

Here is a diagram illustrating the most basic of connections – a user making an HTTP connection to a service on the Internet:

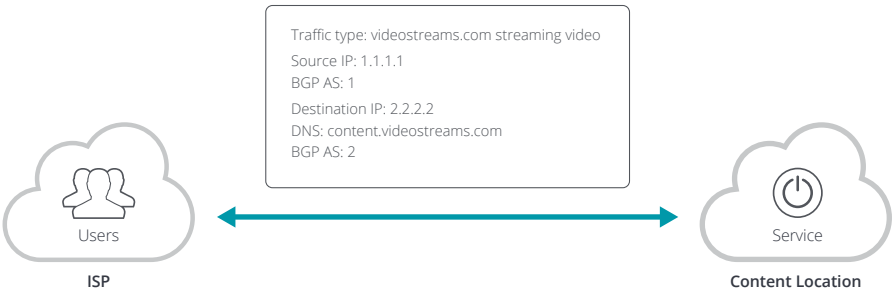


Netflow has provided the 5-tuple information (source and destination ports and addresses as well as the protocol) to Sightline which then correlates it with the routing tables. In combination, we can see who the source and destination organizations are, and the path the traffic is taking. Unfortunately, this provides very little information about the actual content of the traffic or intention of the user.

Without deeper insight, this traffic follows normal routing and peering paths. There is no advanced routing or optimization happening.

How Do We Bring Better Insight Into What Is Going On?

When we combine this information with DNS, we are able to infer a user's intention, and as a result, more intelligently and accurately classify the traffic. This diagram shows the same TCP connection but illuminated by the DNS entry "content.videostreams.com".



Now we can identify and classify this connection as streaming video and not merely HTTP – or more specifically (and less descriptively) as TCP/80. By determining this intent, we can categorize connections between users and services more intelligently. Metering those categorized connections will provide more meaningful information about what is actually happening on the network and how it is being utilized.

"The real bright spot has been our direct-to-consumer business, which is key to the future of our company, and on this anniversary of the launch of Disney+ we're pleased to report that, as of the end of the fourth quarter, the service had more than 73 million paid subscribers – far surpassing our expectations in just its first year," said CEO Bob Chapek in a statement.

https://techcrunch.com/2020/11/12/disney-73-million-subscribers/

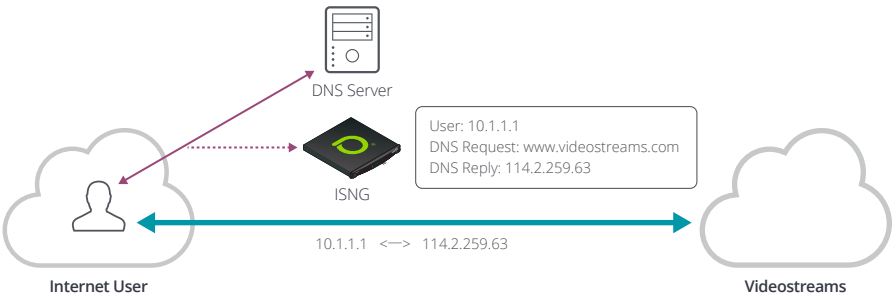
The challenge has become determining what services are actually being utilized when IP addresses or ASNs are not providing enough insight.

Metering DNS information and categorizing the correlated connections provides more meaningful information about user intent, revealing what is actually happening on the network and how it is being utilized.

Where Does the DNS Information Come From, and How Does Sightline Actually Do the Correlation?

ATLAS® Managed Objects (AMOs) are Sightline Managed Objects received through the ATLAS Intelligence Feed (AIF). They contain information to match traffic by criteria such as IP address and DNS. AMOs are categorized and tagged for identifying and classifying traffic into groups such as "CDN" or "streaming" or "collaboration". AMOs are updated as part of the intelligence feed allowing for up-to-date identification.

In conjunction with ATLAS Managed Objects, DNS traffic can be ingested from the wire utilizing an nGenius® InfinistreamNG® (ISNG) appliance which would reside within your network visibility layer. The ISNG receives copies of the network traffic, generating Smart Data based on those traffic flows utilizing its ASI technology. When DNS traffic is seen by the ISNG, the requester's IP address and the DNS name-to-IP response is passed to Sightline. This information is correlated to the subsequent connection that is seen by Sightline through normal flow gathering.

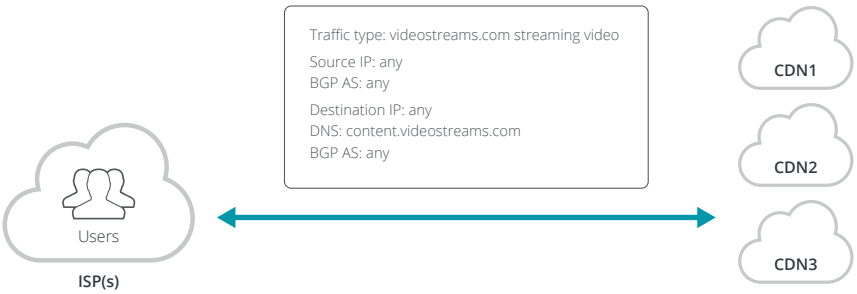


As depicted above, the user at 10.1.1.1 requests DNS resolution for "www.videostreams.com" and the IP address "114.2.259.63" is returned. This information is seen by the nGenius InfiniStreamNG and sent to Sightline. The connection established from the user to www.videostreams.com is now able to be categorized as streaming video.

ATLAS Managed Objects (AMOs) are continually received through the ATLAS Intelligence Feed (AIF) enabling up-to-date identification of OTT traffic.

Looking Beyond the Single Destination

As more users and connections are seen using this DNS name or prefix, we may discover that the content itself is dispersed across multiple locations:



Now "content.videostreams.com" is located in multiple places, some of which might be direct peers.

The IP addresses and BGP AS numbers will be correlated continually and it becomes possible to better see where videostreams.com content resides and subsequently evaluate our routing and peering to optimize that traffic flow.

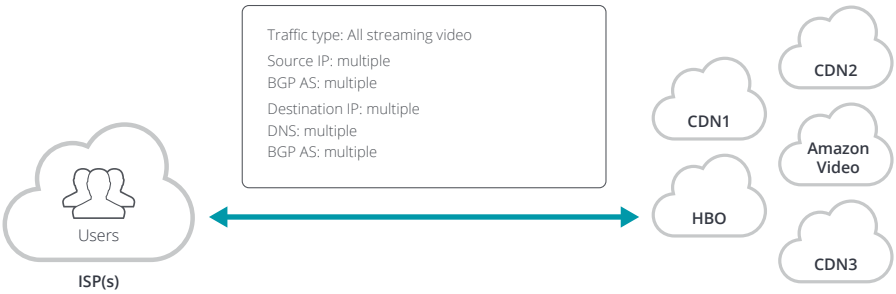
Utilizing DNS gathered by an ISNG and combining that information with AMOs, we are even able to identify multiple services which may reside behind the same IP. For example – an edge caching server might provide content for multiple providers; each uniquely identified by DNS domains. In reality most services are actually farms of servers, load-balanced behind a virtualized IP address (VIP). That single address might reflect a few, dozens, or even hundreds

Smart Data from ISNG + ATLAS Managed Objects = Smart Visibility into OTT Traffic

of services and types of content. This combination of DNS information with Sightline and ATLAS Managed Objects allows us to measure and categorize every flow uniquely, differentiating by content regardless of its location.

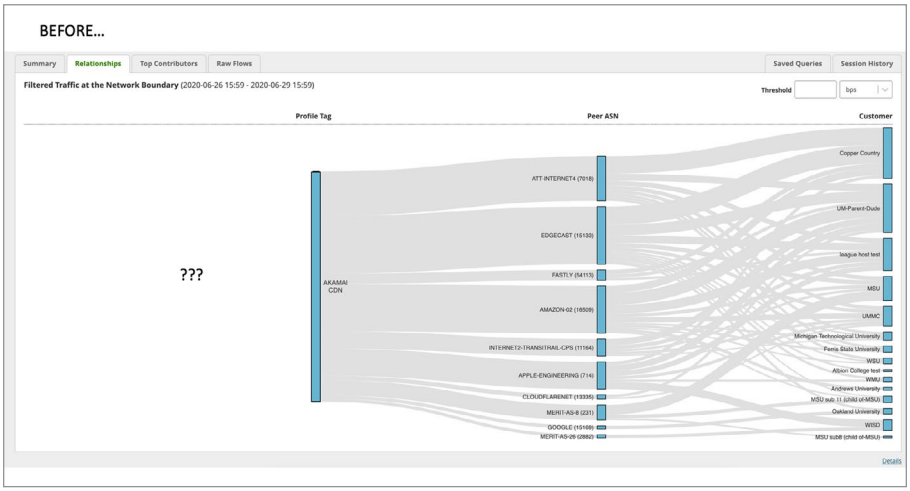
Categorizing Traffic Types and Reporting

Taking a step further back, we can use Sightline's managed objects and tags to see all the streaming video content transiting the network:



Now we are able to view the network traffic flows from the perspective of content.

In the examples below, we can see traffic flows from our customers through our peers and out to the destination. In the BEFORE example, we can see Akamai (CDN) as the destination but cannot determine or classify the traffic in any meaningful way beyond that:

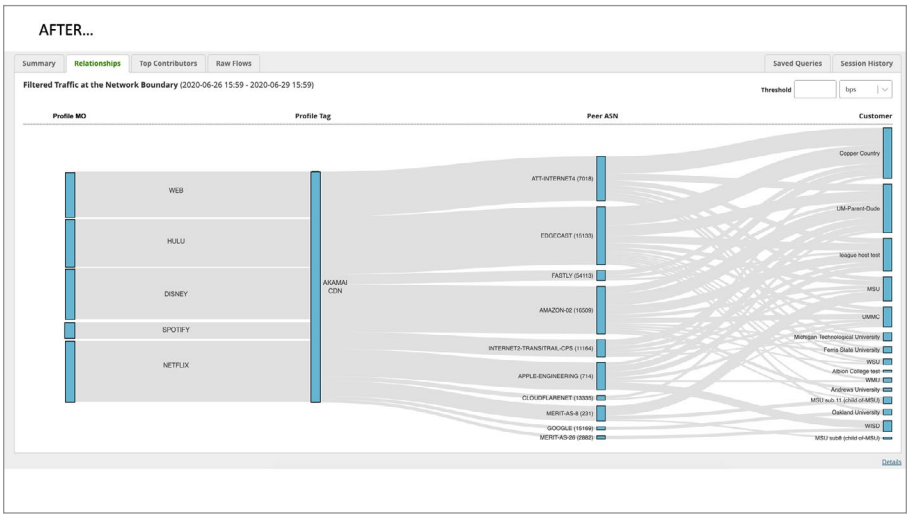


In the AFTER example, Sightline's OTT visibility allows us to now look beyond mere IP and ASN, and see what services users are actually reaching and categorize and report them as they occur:

Arbor Insight Allows you to Understand the Value of Your Connectivity.

Over-The-Top/Content Visibility reveals ambiguous flows to better convey the meaning to traffic beyond CIDR prefixes or ASN to better understand user's intent.

In the AFTER example, Sightline's OTT visibility allows us to now look beyond mere IP and ASN, and see what services users are actually reaching and categorize and report them as they occur:



Clearly there is much more insight available, enabling the network operators to identify and categorize traffic more effectively, and make more informed network design and routing decisions than they were previously able.

Conclusion

Traditional traffic analysis is insufficient in today's networks. The ubiquity and mobility of services means greater insight into traffic loads is necessary for achieving better user experiences and optimizing both costs and peering relationships. Arbor Sightline provides this insight with powerful and flexible reporting, enabling network operators to optimize both the network of today and tomorrow.

LEARN MORE

For more information about Arbor Insight please visit:

www.netscout.com/product/arbor-insight

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECWP_016_EN-2202 08/2022