April 2023

UNKNOWN SERVER NAME INDICATION (SNI) PROCESSING

Bill Cox

Mike Lugo

UNKNOWN SERVER NAME INDICATION (SNI) PROCESSING

AUTHORS:
Bill Cox
Mike Lugo

ABSTRACT

Current methods of server name indication (SNI) detection rely on manual traffic analysis to determine which SNIs should be added to a list of SNIs in Application Detection and Control (ADC) peer-to-peer (P2P) modules, which may lead to errors when determining which traffic should be shaped for optimization. Techniques described herein provide for a robust and quantifiable method of determining which SNI traffic flows should be shaped or optimized in a Service Provider's mobile packet core. Techniques discussed herein reduce the time to identify flows requiring actions and make the process of identifying the flows more quantifiable with live unknown traffic monitoring.

DETAILED DESCRIPTION

The SNI detection included in ADC P2P modules takes too long to get updated and relies on manual traffic analysis to determine which SNIs should be added. The current method leaves room for error as to what traffic should be shaped for optimization. The long time to update the P2P module has been resolved by allowing manual configuration, but the manual configuration does not help in identifying which SNIs should be detected and optimized.

SNI allows multiple secure websites to be served from the same Internet Protocol (IP) address without requiring all the sites to use the same certificate. SNI provides a mechanism that allows the client to tell the server to which hostname the client is trying to connect. ADC detects encrypted traffic using the SNI field/signatures of Transport Layer Security (TLS)/ Secure Sockets Layer (SSL) traffic and the signatures are added to a plugin. Any new SNI fields in the already detected applications or new applications are added to the plugin and a new version of the plugin is released. Frequent releases of plugin versions cause a delay in upgrading the new plugin in the network and lead to revenue leak to the operator. Due to an increased number of applications moving towards TLS/SSL, the SNI may be configured in ruledef and traffic may be classified based on the configured SNI.

When large events (e.g., sporting events, concert events, etc.) are taking place, customers may stream the events using online streaming services. The additional traffic may strain packet core gateways and the SNIs associated with the online streaming services should be added to the list of known SNIs for detecting and shaping. In one instance, when a large number of customers were streaming a large, multi-day event over an online streaming service, a new P2P module including the SNIs associated with the online streaming service was ordered. While waiting on delivery of the new P2P module, flows that were thought to be unshaped flows associated with the online streaming service were detected and the update to the P2P was canceled. Further analysis of the traffic showed that the additional flows were not flows associated with the online streaming service. If Unknown SNI processing had been in place, it would have been faster to determine that the online streaming service flows needed to be shaped. In addition, the additional SNIs might have been shaped if needed.

Figure 1, below, illustrates an example of current SNI processing.

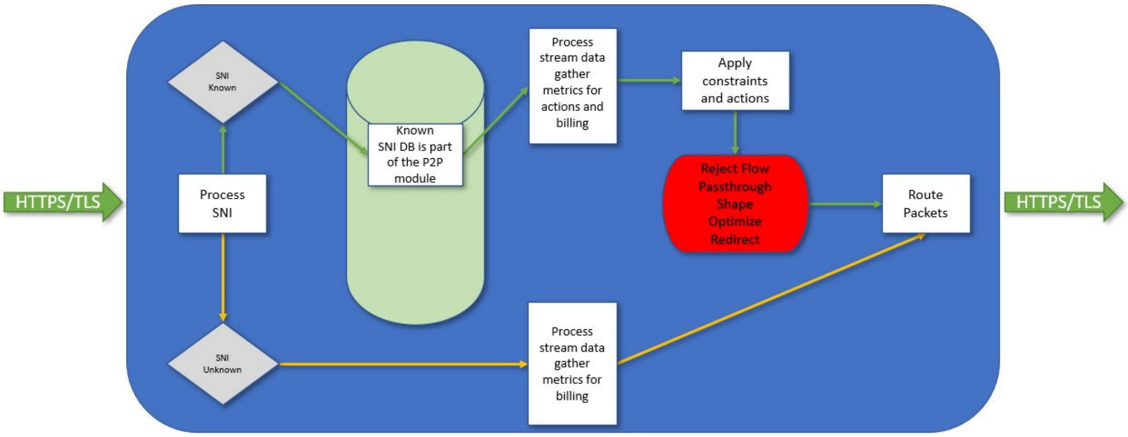

HTTPS/TLS
Process SNI
SNI Known
SNI Unknown
Known SNI DB is part of the P2P module
Process stream data gather metrics for actions and billing
Apply constraints and actions
Reject Flow
Passthrough
Shape
Optimize
Redirect
Route Packets
Process stream data gather metrics for billing
HTTPS/TLS

Figure 1: Example Diagram of SNI Processing

In many traffic detection processing features, a known list of aspects to detect is a subset of the actual traffic flows. Those known aspects are then acted upon once detected.

Actions vary from triggering other actions, dropping, shaping, redirecting, rate limiting, etc.

Techniques described herein explore the unknown side of traffic detection with a specific aspect currently used in mobility products - the SNI. Figure 2, below, illustrates an example of unknown SNI processing.

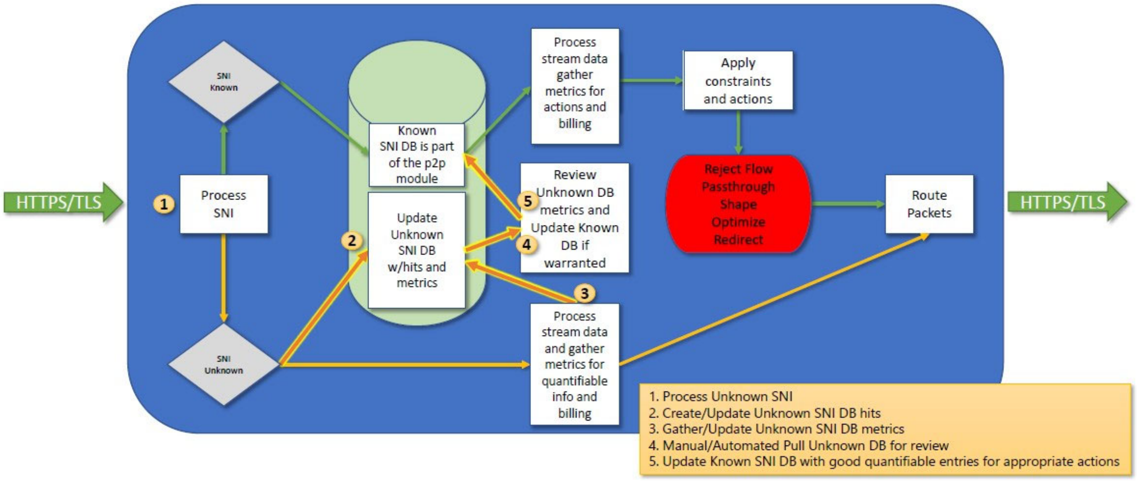
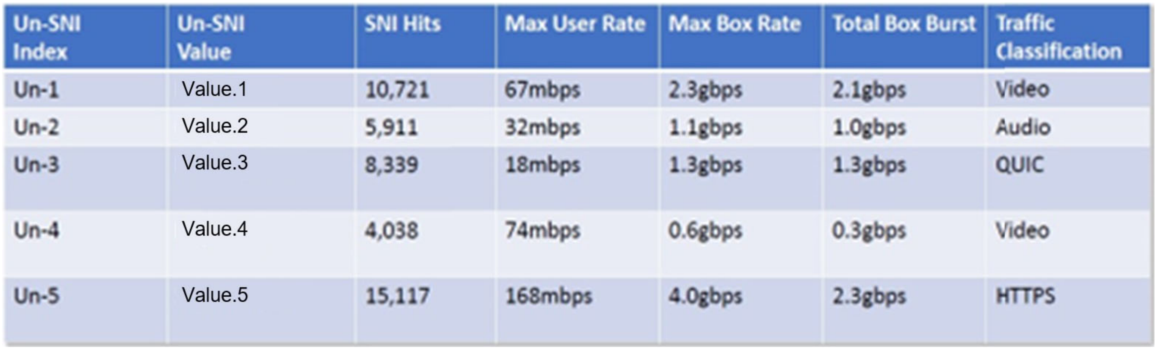

HTTPS/TLS
1
Process SNI
SNI Known
SNI Unknown
Known SNI DB is part of the p2p module
2
Update Unknown SNI DB w/hits and metrics
Process stream data gather metrics for actions and billing
5
Review Unknown DB metrics and Update Known DB if warranted
4
3
Process stream data and gather metrics for quantifiable info and billing
Apply constraints and actions
Reject Flow
Passthrough
Shape
Optimize
Redirect
Route Packets
HTTPS/TLS
1. Process Unknown SNI
2. Create/Update Unknown SNI DB hits
3. Gather/Update Unknown SNI DB metrics
4. Manual/Automated Pull Unknown DB for review
5. Update Known SNI DB with good quantifiable entries for appropriate actions

Figure 2: Example Diagram of Unknown SNI Processing

As described in Figure 2, while the known SNI detection is taking place, unknown SNI processing will identify and log to a database all the traffic destined to unknown SNIs. Figure 3, below, illustrates an example unknown SNI database with mock metrics. Metrics in the database may vary based on SP requirements.



Un-SNI Index	Un-SNI Value	SNI Hits	Max User Rate	Max Box Rate	Total Box Burst	Traffic Classification
Un-1	Value.1	10,721	67mbps	2.3gbps	2.1gbps	Video
Un-2	Value.2	5,911	32mbps	1.1gbps	1.0gbps	Audio
Un-3	Value.3	8,339	18mbps	1.3gbps	1.3gbps	QUIC
Un-4	Value.4	4,038	74mbps	0.6gbps	0.3gbps	Video
Un-5	Value.5	15,117	168mbps	4.0gbps	2.3gbps	HTTPS

Figure 3: Example Unknown SNI Database

As multiple subscribers set up flows to the unknown SNI, a tally of the number of hits and packet rates to these newly learned SNIs will be added to the database. As time goes on, the database will contain the information needed for administrators to make decisions on which SNIs should be moved to the detect list and which actions and billing are to be taken with respect to traffic flowing to and from those SNIs. Techniques described herein provide for a proactive approach to identifying new SNIs that allows operators to take action based on the amount of traffic visiting those unknown SNIs. Unknown traffic processing builds a more robust and quantifiable SNI detection list and gives operators an indication of potential traffic that might need optimization, special billing, redirection, or rerouting.

To summarize, according to techniques provided herein, unknown SNI processing is a robust and quantifiable method of determining which HTTPS/TLS SNI traffic flows should be shaped or optimized in a Service Provider's 4G/5G Mobile Packet Core. This proactive approach helps signaling points reduce the time to identify flows that require action and makes the process of identifying the flows more quantifiable with live unknown traffic monitoring.