April 2022

METHOD FOR THE EFFECTIVE UTILISATION OF THE TUNNEL BETWEEN SDWAN ROUTER AND SECURE INTERNET GATEWAY

Niranjan M M

Vijay Kothamasu

Nagaraj Kenchaiah

METHOD FOR THE EFFECTIVE UTILISATION OF THE TUNNEL BETWEEN SDWAN ROUTER AND SECURE INTERNET GATEWAY

AUTHORS:
Niranjan M M
Vijay Kothamasu
Nagaraj Kenchaiah

ABSTRACT

With the integration of SD-WAN and third-party SIG, all the traffic from the enterprise client's is forwarded to the SIG over the tunnel. The SD-WAN router at branch office is connected to the SIG over WAN link. Hence there are always bandwidth (aka throughput capacity) limitations for the traffic being routed over the tunnel. For the same reason, service providers would enforce limitations on throughput capacity per tunnel basis. In view of this fact, the effective usage of the link between SD-WAN router and SIG is essential. Also, SD-WAN has enabled customers to prioritize cloud applications and deliver better application performance to their branch network for an always-connected workplace. In fact, SD-WAN helps for the efficient use of the bandwidth from branch locations. As the number of clients and services are ever increasing, there is every need to further optimize the usage of the link between SD-WAN at branch location to the SIG and/or cloud services. The techniques presented herein propose method to consider optimizing the traffic flowing between SD-WAN router and SIG to efficiently utilize the limited tunnel bandwidth available using consolidation, compression, and aggregation methods.

DETAILED DESCRIPTION

Enterprise SD-WAN deployments would be having multiple branch routers which are Software-Defined branch (SD-Branch) routers. SD-Branch is a branch router that supports SD-WAN routing, security and other LAN access features that can be managed centrally. A thick branch is a high-end device that can incorporate all these features and provide required scale and performance for large enterprises. However, on a lean branch not all security features can be switched on. These branch routers can integrate with third party Secure Internet Gateways (SIG)

for securing the enterprise traffic. In general SIG provides services such as DNS, web proxy and other internet services.

The Direct Internet Access (DIA) ingress traffic on SD-WAN service VPN's may be tunnelled to SIG's for securing enterprise traffic. All LAN/Wi-Fi enabled enterprise client's traffic, based on routing or policy, will be forwarded to the SIG. In addition, SIG protects roaming/mobile users, BYOD use-cases as well. To achieve the same, SD-WAN branch/edge router creates IPSec/GRE tunnels to the SIG (a cloud-based security application stack) and locally breaking out internet bound packets from multiple service VPNs to this SIG through IPSec/GRE tunnel established, after which they carry on towards their actual destinations. The return traffic is de-multiplexed back to the source VPNs.

With the integration of SD-WAN and third-party SIG, all the traffic from the enterprise client's is forwarded to the SIG over the tunnel. The SD-WAN router at branch office is connected to the SIG over WAN link. Hence there are always bandwidth (aka throughput capacity) limitations for the traffic being routed over the tunnel. For the same reason, service providers would enforce limitations on throughput capacity per tunnel basis. In view of this fact, the effective usage of the link between SD-WAN router and SIG is essential. Any such effort would help in carrying the information of more client's traffic with same link capacity.

SD-WAN has enabled customers to prioritize cloud applications and deliver better application performance to their branch network for an always-connected workplace. In fact, SD-WAN helps for the efficient use of the bandwidth from branch locations. As the number of clients and services are ever increasing, there is every need to further optimize the usage of the link between SD-WAN at branch location to the SIG and/or cloud services. One such prominent service is DNS server hosted in the cloud. Client's DNS traffic gets channelized from SD-WAN to the DNS SIG. Statistics indicate DNS traffic is significant in overall internet traffic and percentage is ever increasing in proportionate to cloud hosted internet services.

. The techniques presented herein propose method to consider optimizing the traffic flowing between SD-WAN router and SIG to efficiently utilize the limited tunnel bandwidth available using consolidation, compression, and aggregation methods. As an example, this proposed method

considers optimizing the flow of the DNS traffic between SD-WAN router and DNS server on the SIG. In other words, this method optimise the DNS traffic sent over the IPSec/GRE tunnel along with ensuring client/user policies are conveyed end-to-end. By the nature of DNS requests and responses (based on content and its type), here are few methods where DNS traffic can be optimized.

A. Combining DNS requests and DNS responses:

In a typical deployment there will be several thousands of clients present behind SD-WAN router, each will be sending the DNS requests to DNS SIG along with specific policy tags (aka EDNS records). SD-WAN router being the common point of traversal for these packets, it is possible to combine these individual packets in a consolidated manner. Except client's detail and EDNS records most of the other fields of the DNS packet are same. Hence multiple such requests can be consolidated into a single packet (custom DNS packet) and can be sent over the tunnel. On the receiving end, this consolidated packet will be converted back into individual DNS request packets and delivered onto the network. In the similar manner, DNS responses also can be consolidated and processed in the return path. Since EDNS record of each client is carried end-to-end, client/user policies are ensured. In short, this method consolidates individual DNS requests and responses into a single packet, thus reduce the overhead of sending individual DNS packets as well as the overhead of the tunnel headers. The consolidated packets carry client specific EDNS records to be used to apply respective user/client policies at the DNS SIG.

For example: Let us say, at a particular time, 10 clients sending DNS query to the DNS SIG to resolve www.example.com via SD-WAN Router. Instead of sending 10 individual DNS queries to resolve www.example.com, SD-WAN router sends only one DNS query to the DNS SIG over the tunnel. To have the policy-based access, EDNS record of each client would also be sent in consolidated custom DNS request packet.

DNS SIG apply the policy based on the EDNS record of the client and can have two possibilities:

i. Send the DNS response with the resolved IP address of the www.example.com received in the DNS query request.
ii. Send the URL of the block page (such as https://1.2.3.4) in the DNS response for those clients where www.example.com is blocked based on policy.

In the return path, DNS responses can also be consolidated into single custom response packet from DNS SIG to the SD-WAN router over the tunnel. In the worst case, there would be two DNS responses possible (one with resolved IP address and another with URL of the blocked page).

Figure-1 depicts the consolidated DNS traffic flowing between SD-WAN router and DNS SIG.

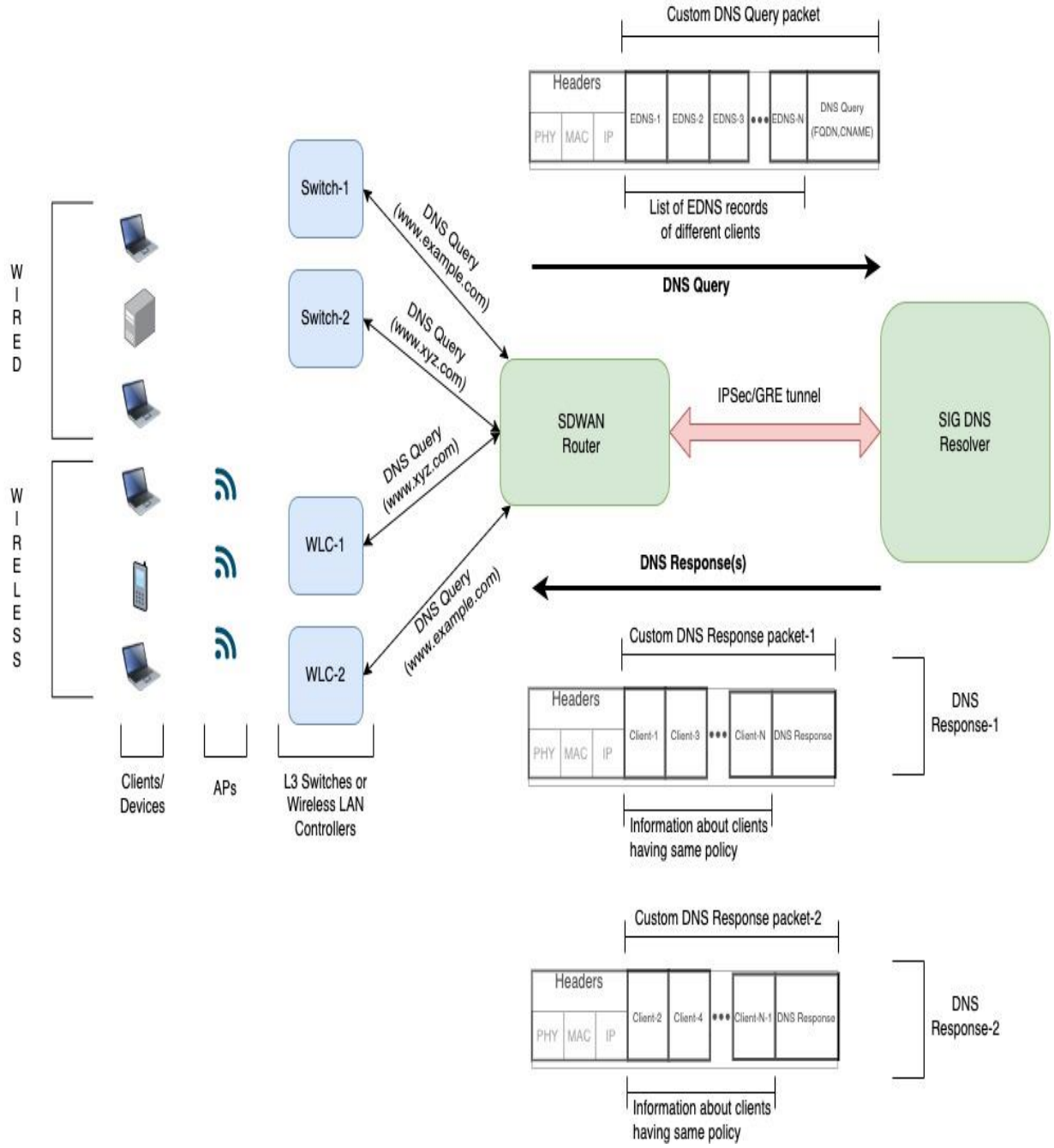

Figure-1

Figure-2 depicts, Custom DNS Query packet with list of EDNS records.

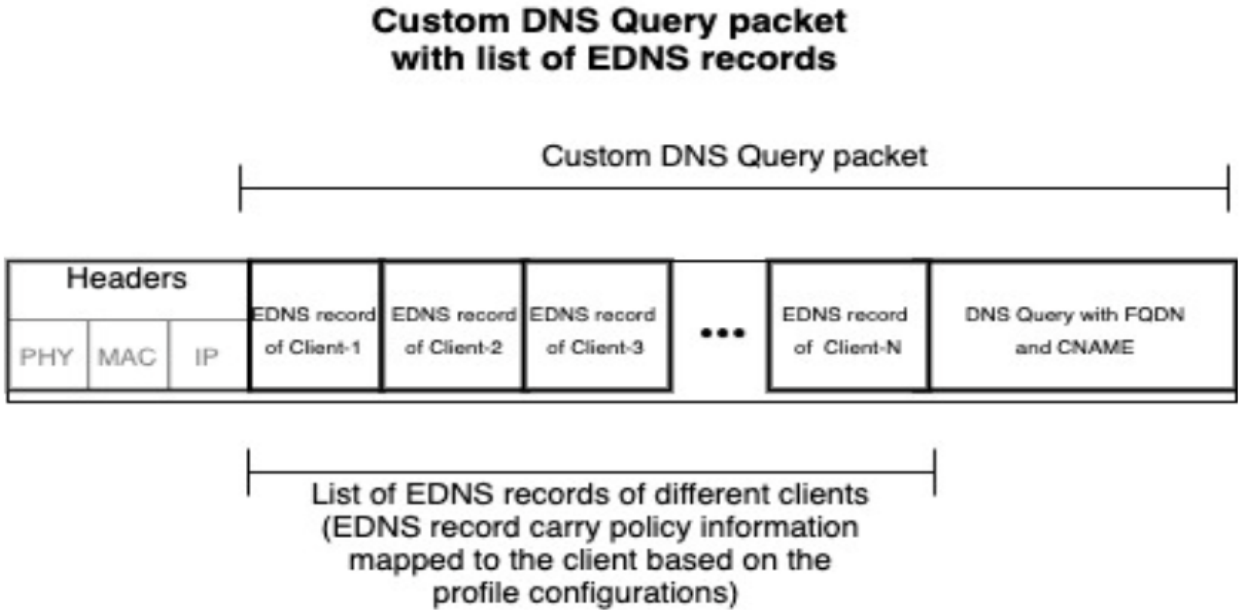

Figure-2

Figure-3 depicts, Custom DNS Response packet with list of client's details.

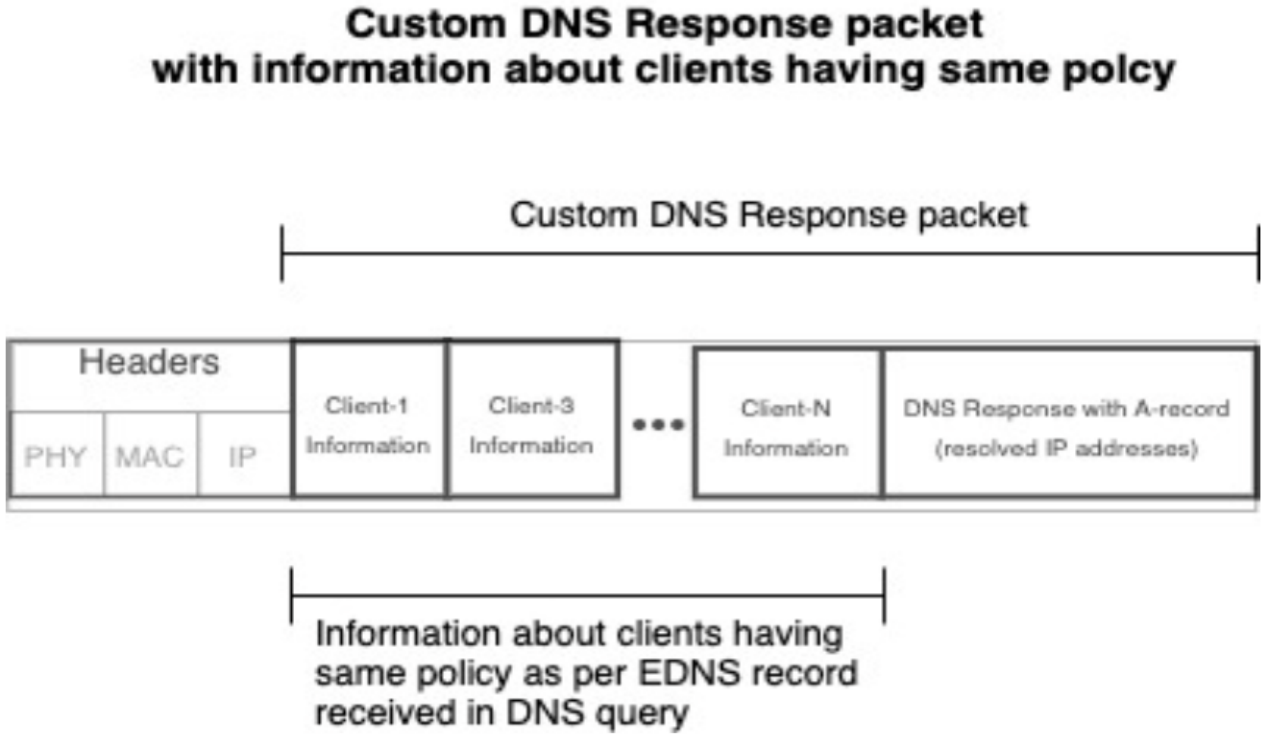

Figure-3

B. Caching the DNS responses:

As per this method, DNS responses (for the FQDN/URLs) can be cached on the SD-WAN router, and it will register for updates of these entries with DNS SIG. Thus, we can avoid forwarding the DNS queries from the clients to the DNS SIG and can be responded with the DNS response at the SD-WAN router itself. This will ensure responses are quick and avoids sending them over tunnel. The number of entries to be cached are limited by the platform type. There can be user defined criteria as which type of entries to be cached. Below are some of the criteria and admin configured will have top priority, (i) User policy (ii) Specific FQDNs, (iii) Max hits (most frequently used). In short, this method uses SD-WAN router to cache the DNS responses based on pre-defined criteria and minimize the traffic on the tunnel, also provide better quality of service as request are handled locally.

C. Compression of DNS packets:

DNS packets especially the responses contain domain names, cnames which are ASCII based data. Compression algorithms are very effective on the ASCII data to give better yield and reduce the packet size. Along with the existing compression methods mentioned in RFC8618, RFC1035, standard algorithms suitable for ASCII data compression shall be used. In short, this method applies compression algorithms on DNS packets to compress them further before sending over the tunnel.

D. Aggregation of the DNS packets:

The consolidated and compressed packets are further aggregated into a single packet up to the max size of MTU. This will minimize the overhead due to the tunnel headers. Some of the standard aggregation methods shall be used in this scenario.

Figure-4 depicts the aggregation of compressed DNS packets flowing between SD-WAN router and DNS SIG.

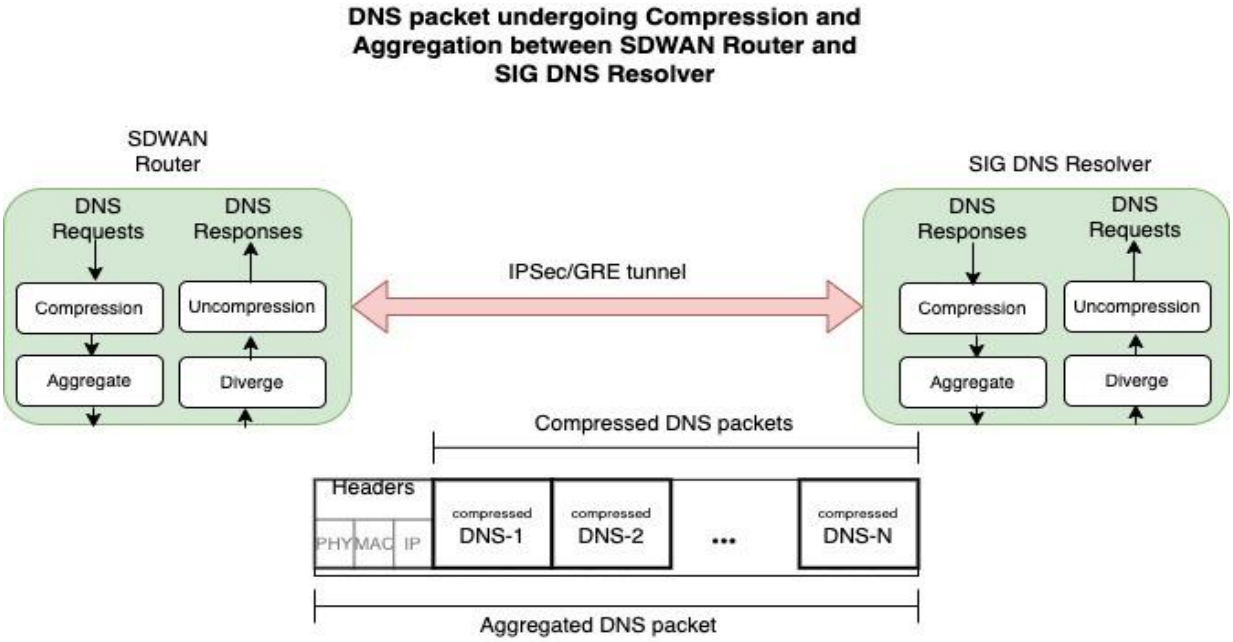

Figure-4

In short, this method applies the standard aggregation techniques on the combined and compressed DNS packets before sending over the tunnel, so that overhead due to tunnel headers shall be minimized to a large extent.

The techniques presented herein is explained in detail as below.

- SD-WAN router would receive DNS query packets from multiple clients.
- Multiple DNS query packets from clients having the same FQDN can be consolidated into a single packet along with EDNS records of each client.
- Apply the compression techniques to reduce the size of the consolidated DNS packet.
- Aggregate the compressed packets up to the max of MTU in each time and send it over the tunnel.
- On the receiving side, SIG will split into multiple packets, un-compress and convert them into multiple individual DNS query packets and deliver them on to the network.
- In the return path, DNS responses are also applied with the same techniques to combine multiple DNS responses into a consolidated custom packet, compressing it, aggregating it and send back over the tunnel to SD-WAN.

- On receiving the packet SD-WAN router will do the reverse process to split into individual DNS response packets and deliver them on the clients.
- SD-WAN routers can also selectively cache some of these DNS responses based the admin defined criteria.

The techniques presented herein increase the effective usage of the WAN link between SD-WAN router and SIG. Moreover, this method is applicable for DNS SIG, Secure Web Gateway (SWG) and applicable for any third-party SIG.

Appendix-A:

Following are some of the factors why DNS traffic will give better results with compression and aggregation:

- DNS packets contain lot of ASCII data due to which compression will be more effective.
- DNS packets are in general small, if we send these packets individually, tunnel header overhead on each packet will be really taxing. This will reduce effective bandwidth of the link.
- With the increased cloud services, DNS traffic is also increasing proportionately, hence it is essential to optimize them.
- Due to small size of the packets, aggregation will be more effective and help to minimize the impact of the overhead due to tunnelling.

Appendix-B:

A sample calculation as how much bandwidth will be saved: Considering MTU of 1500.

- IPSec Header for each packet [20-byte new IP header + 8 Bytes of new UDP + 16 Byte ESP Header + 2 Byte ESP Trailer + 12-byte ESP Authentication data] = ~ 58 bytes.
- Around 1400 bytes of payload - A consolidated packet can carry 10 to 15 DNS queries approx. With compression this count will increase further.
- With existing method: For 10 packets => 10(packets) * 58(ipsec headers) + 10 * 120(average DNS packet size) = 1780 bytes.
- With proposed method = 58 + 10 * 120 = 1258 bytes
- 30% of bandwidth saving with a smaller number of packets to be encrypted.