

ABSTRACT

A method and an electronic device for traffic tunneling in a distributed network for detecting malicious content are provided. The method comprises: transmitting, to a central server, a request for receiving a gateway data from a given gateway; in response to receiving the gateway data, adding the given gateway as a peer to a WireGuard interface of an electronic device; transmitting, to the central server, an Address Resolution Protocol (ARP) probe which is indicative of whether the electronic device is ready to establish a p2p connection with the given gateway; in response to receiving a response to the ARP probe, updating the gateway data in a neighbor table hosted on the given emitter; transmitting an outgoing traffic packet to the given gateway for natting; in response to receiving, from the given gateway, an incoming traffic packet, analyzing a content of the incoming traffic packet for maliciousness.

Fig. 1