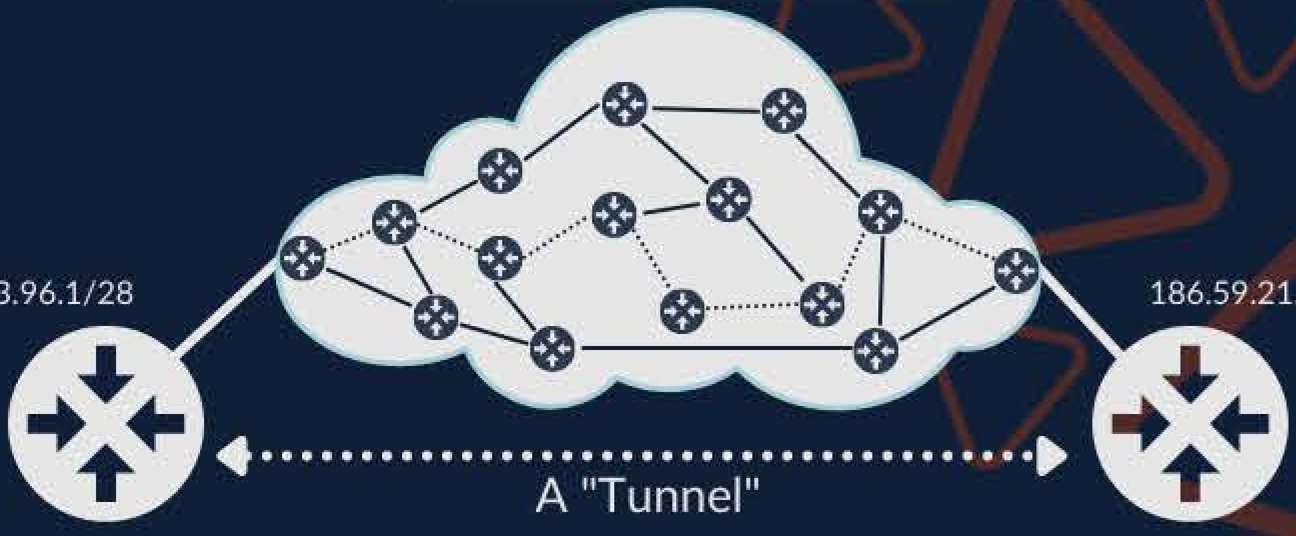
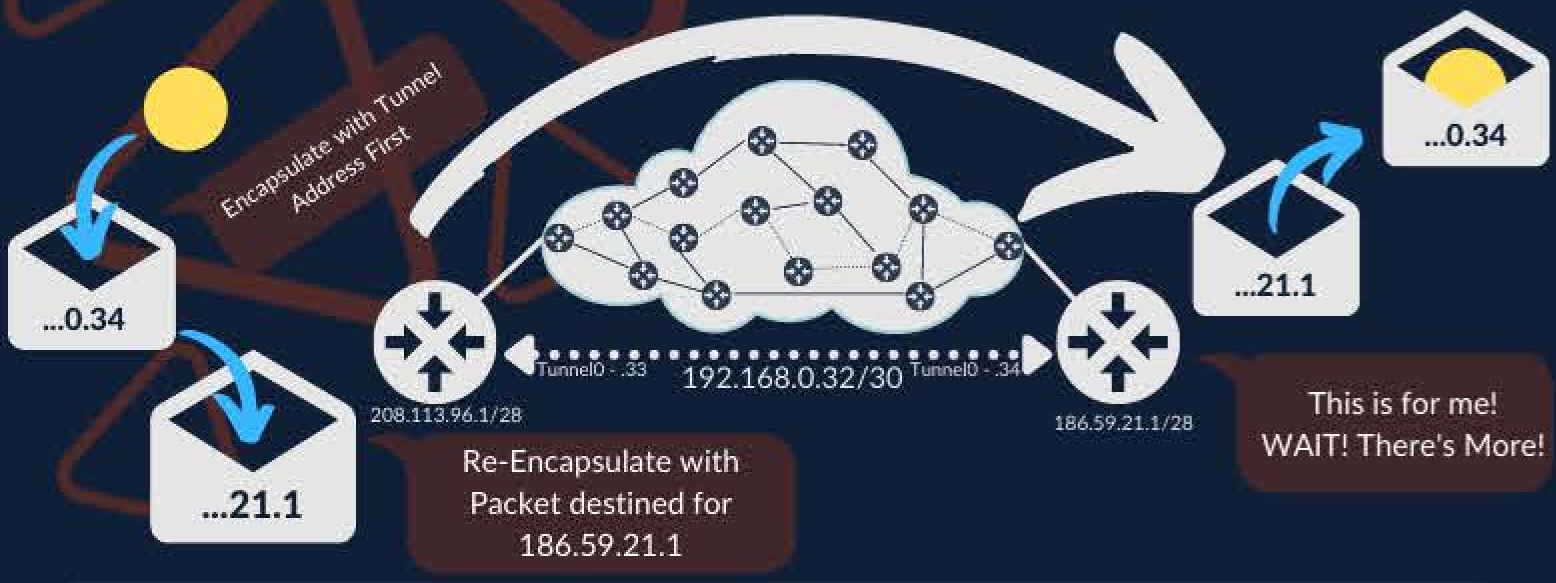
THE LOGIC BEHIND
Site-to-Site VPNs

NOTE: This is NOT Network Address Translation (NAT).

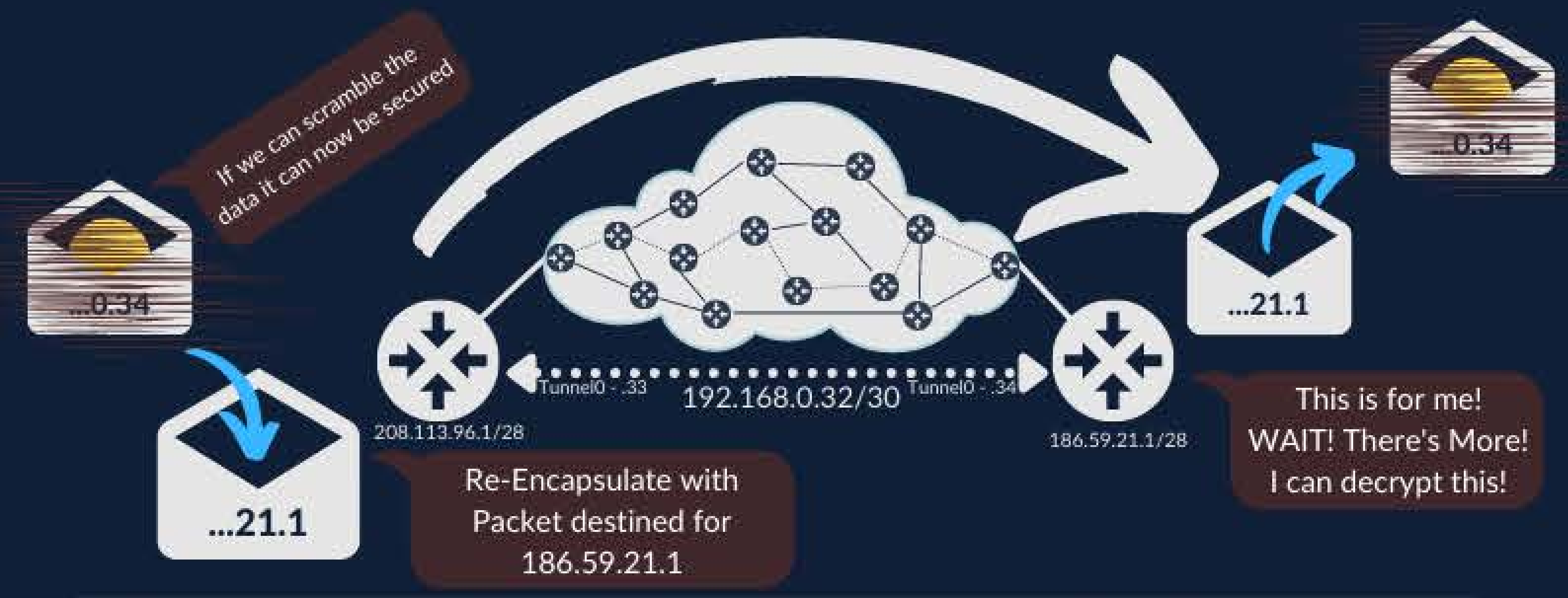


A common misconception with beginners is that once a tunnel is created traffic no longer goes through the internet to get to the remote destination on the other side. The trick is Encapsulation

(To keep this simple) The data we want to send will be at one point be encapsulated into a "Packet". This packet includes the destination logical public addresses, and will be routed over the internet along any viable path.



When we send over a tunnel, RE-ENCAPSULATION is key.
As far as all other routers in the cloud are concerned they only see the Public destination address. Only upon arrival is the packet opened and the Private Tunnel information is displayed.



Next, secure the data. This is done via encryption. Our routers will likely have a secure password configured for encrypting and decrypting. Some tools encrypt the data only, others include the packet information as well. If a packet is intercepted, the data cannot be read without the decryption password.
All of this creates the illusion of a point to point connection. Even though we still traverse the internet via any viable path.