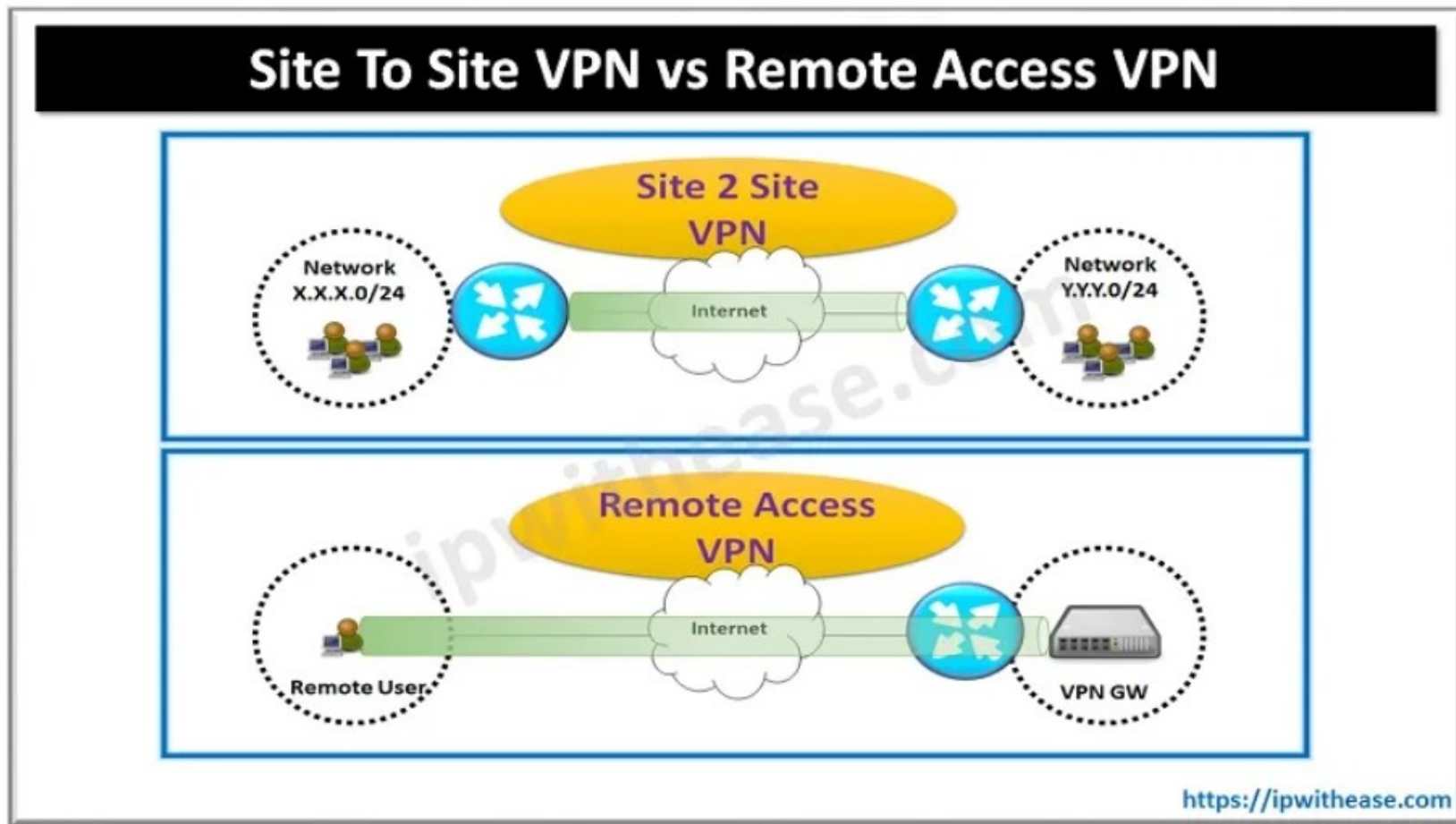


# VPN (Virtual Private Network)

Michele Stecca Ph.D.

# Site 2 Site vs. Remote Access VPN



# DID YOU KNOW?

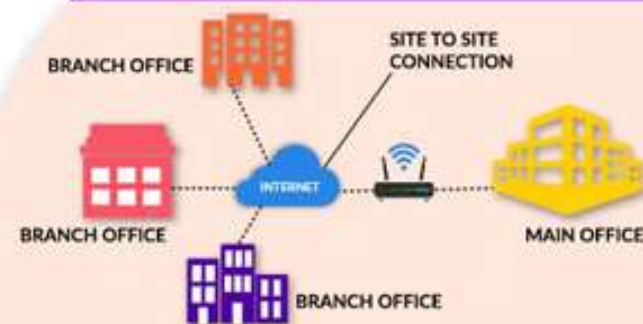
## Type of VPN:

### Remote Access VPN



Remote access VPN allows a user to connect to a private network and access its services and resources remotely. The connection between the user and the private network happens through the Internet.

### Site - to - Site VPN



A Site-to-Site VPN is also called as Router-to-Router VPN and is mostly used in the corporates. Companies, with offices in different geographical locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.



VPN



<https://www.servercake.blog>



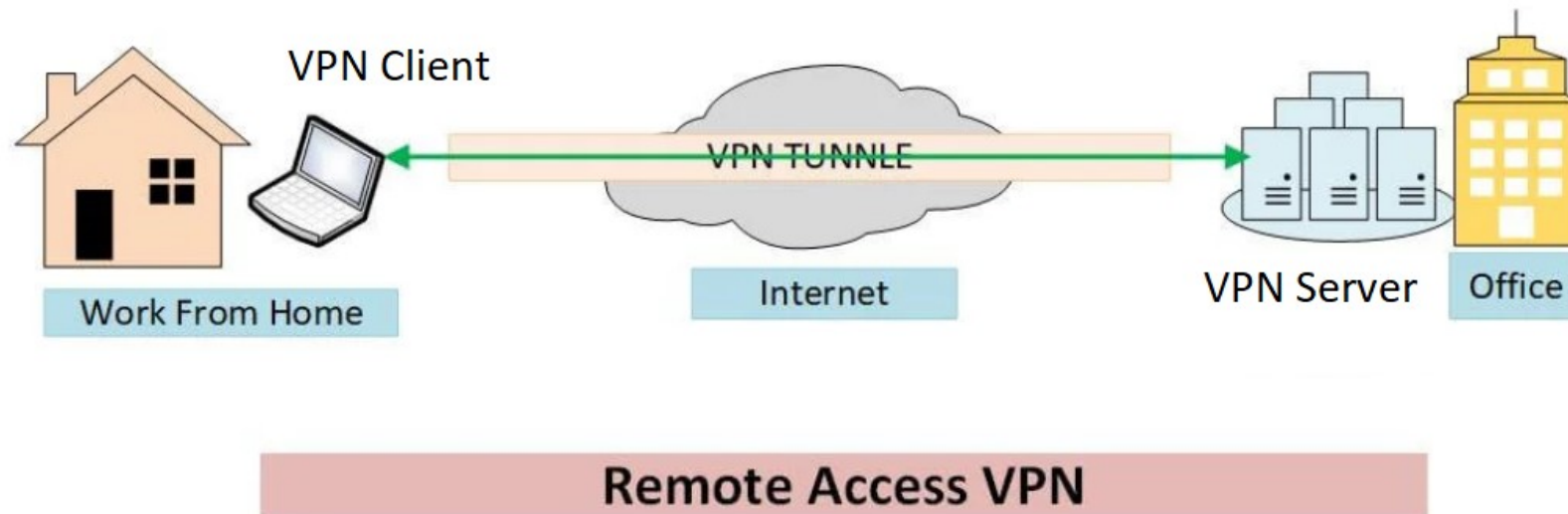
## Site 2 Site vs. Remote Access VPN

| Remote-Access VPN   | Site-to-Site VPN  |
|---|---|
| In Remote-Access VPN, a client software is used on the user's device.                         | In Site-to-Site VPN, no client software is needed on the user's device.   |
| In Remote-Access VPN, the user needs to initiate the VPN tunnel setup.                        | In Site-to-Site VPN, the user does not need to initiate the VPN tunnel setup.   |
| In Remote-Access VPN, the user's device communicates with the VPN gateway using a VPN tunnel. | In Site-to-Site VPN, the VPN gateway from one LAN communicates with the VPN gateway of another LAN and creates secure VPN tunnel. |

# Wireguard

(Remote Access)

# Remote Access



Source: <https://www.networkingsignal.com/what-is-a-remote-access-vpn-and-how-does-it-work/>

# Wireguard (Configuration file)

[Interface]

PrivateKey = ALrXXXXXXXXXXXXXXXXXXXXXXXXXXXXE1I=

Address = 10.0.0.6/24 **Virtual Interface**

[Peer]

PublicKey = tLZzINwXXXXXXXXXXXXXXXXXXXXnE4CWlhnymFk=

PreSharedKey = ycSwXXXXXXXXXXXXXXXXXXXXXXXXDpFH0XUOU=

AllowedIPs = 192.168.19.0/24 **Target Network**

Endpoint = 151.69.121.221:1194 **Public Address of VPN Server**

## Keep connection alive ##

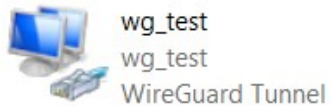
PersistentKeepalive = 30

# VPN activation (client side)

## IPv4 Route Table

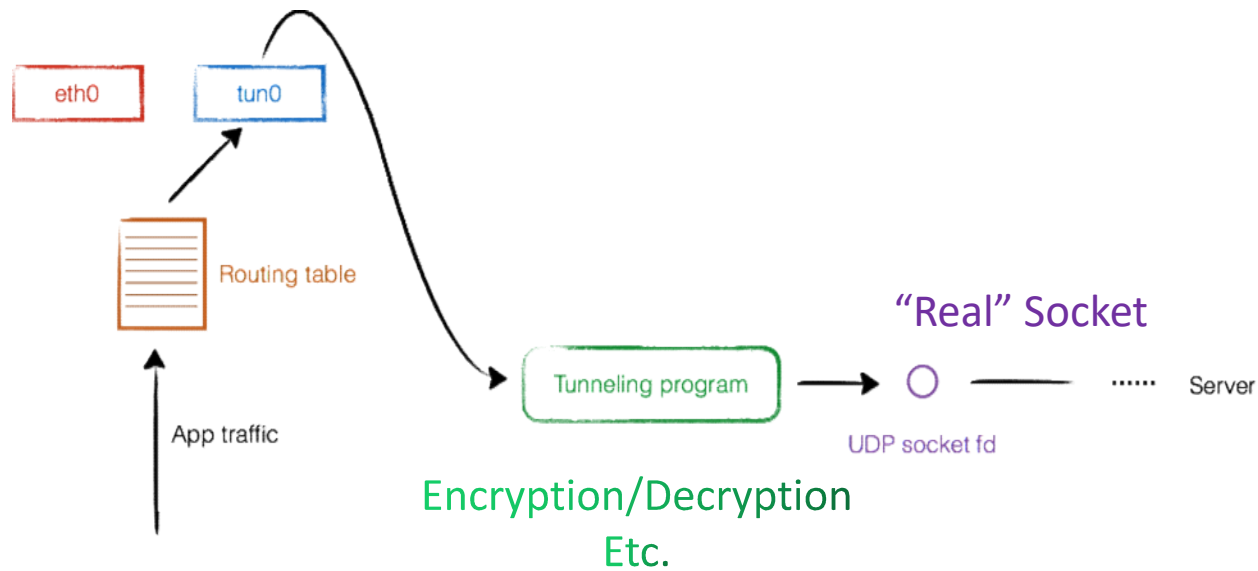
### Active Routes:

| Network | Destination     | Netmask         | Gateway        | Interface       | Metric |
|---------|-----------------|-----------------|----------------|-----------------|--------|
|         | 0.0.0.0         | 0.0.0.0         | 192.168.179.86 | 192.168.179.231 | 55     |
|         | 10.0.0.0        | 255.255.255.0   | On-link        | 10.0.0.6        | 261    |
|         | 10.0.0.6        | 255.255.255.255 | On-link        | 10.0.0.6        | 261    |
|         | 10.0.0.255      | 255.255.255.255 | On-link        | 10.0.0.6        | 261    |
|         | 127.0.0.0       | 255.0.0.0       | On-link        | 127.0.0.1       | 331    |
|         | 127.0.0.1       | 255.255.255.255 | On-link        | 127.0.0.1       | 331    |
|         | 127.255.255.255 | 255.255.255.255 | On-link        | 127.0.0.1       | 331    |
|         | 192.168.19.0    | 255.255.255.0   | On-link        | 10.0.0.6        | 5      |
|         | 192.168.19.255  | 255.255.255.255 | On-link        | 10.0.0.6        | 261    |
|         | 192.168.179.0   | 255.255.255.0   | On-link        | 192.168.179.231 | 311    |
|         | 192.168.179.231 | 255.255.255.255 | On-link        | 192.168.179.231 | 311    |
|         | 192.168.179.255 | 255.255.255.255 | On-link        | 192.168.179.231 | 311    |
|         | 224.0.0.0       | 240.0.0.0       | On-link        | 127.0.0.1       | 331    |
|         | 224.0.0.0       | 240.0.0.0       | On-link        | 192.168.179.231 | 311    |
|         | 255.255.255.255 | 255.255.255.255 | On-link        | 127.0.0.1       | 331    |
|         | 255.255.255.255 | 255.255.255.255 | On-link        | 192.168.179.231 | 311    |





# TUN (Virtual Interface)



Source: <https://lxd.me/a-simple-vpn-tunnel-with-tun-device-demo-and-some-basic-concepts>

Bonus: OpenVPN

<https://www.youtube.com/watch?v=4ykbyOEsKQE>

# IPSec

(Site-2-site)

# IPSec: some protocols

## Internet Key Exchange (IKE)

Creates and maintains IKE SAs and IPsec SAs, including the following functions:

- Negotiates protocol parameters (encryption and authentication protocols).
- Authenticates peer identities.
- Negotiate and manages keys.

## Authentication Header (AH)

## Encapsulating Security Payload (ESP)

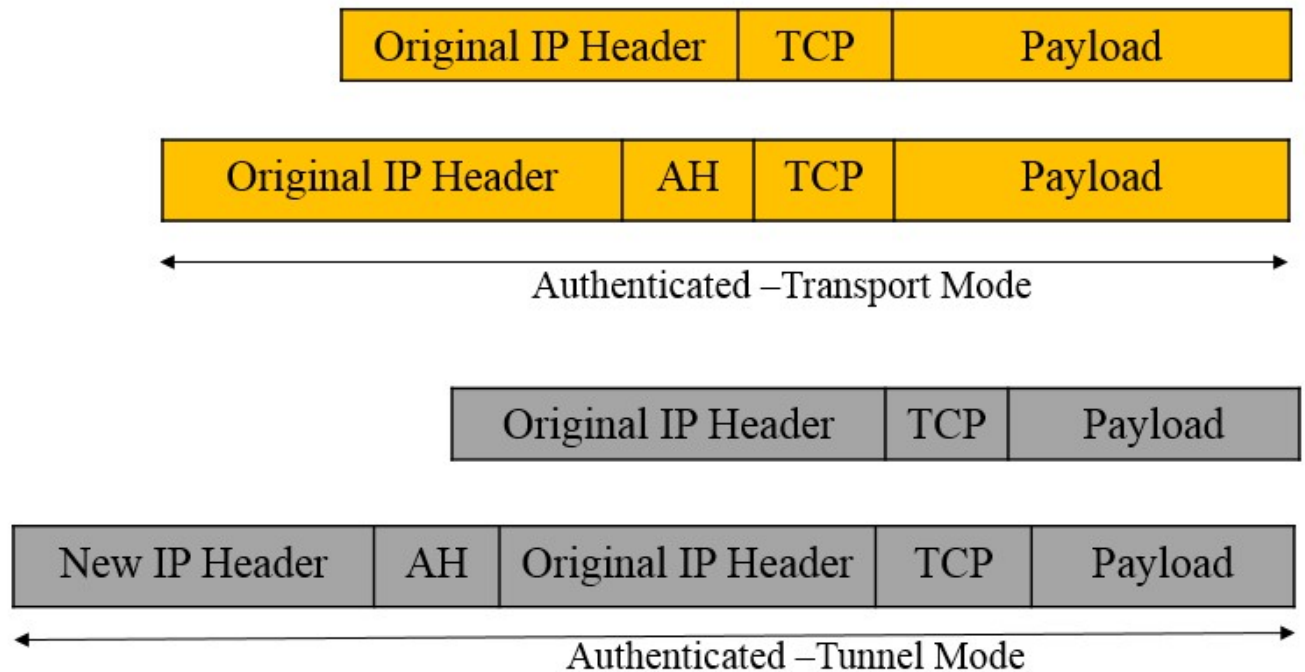
Security protocols that protect traffic.

Authentication  
algorithm

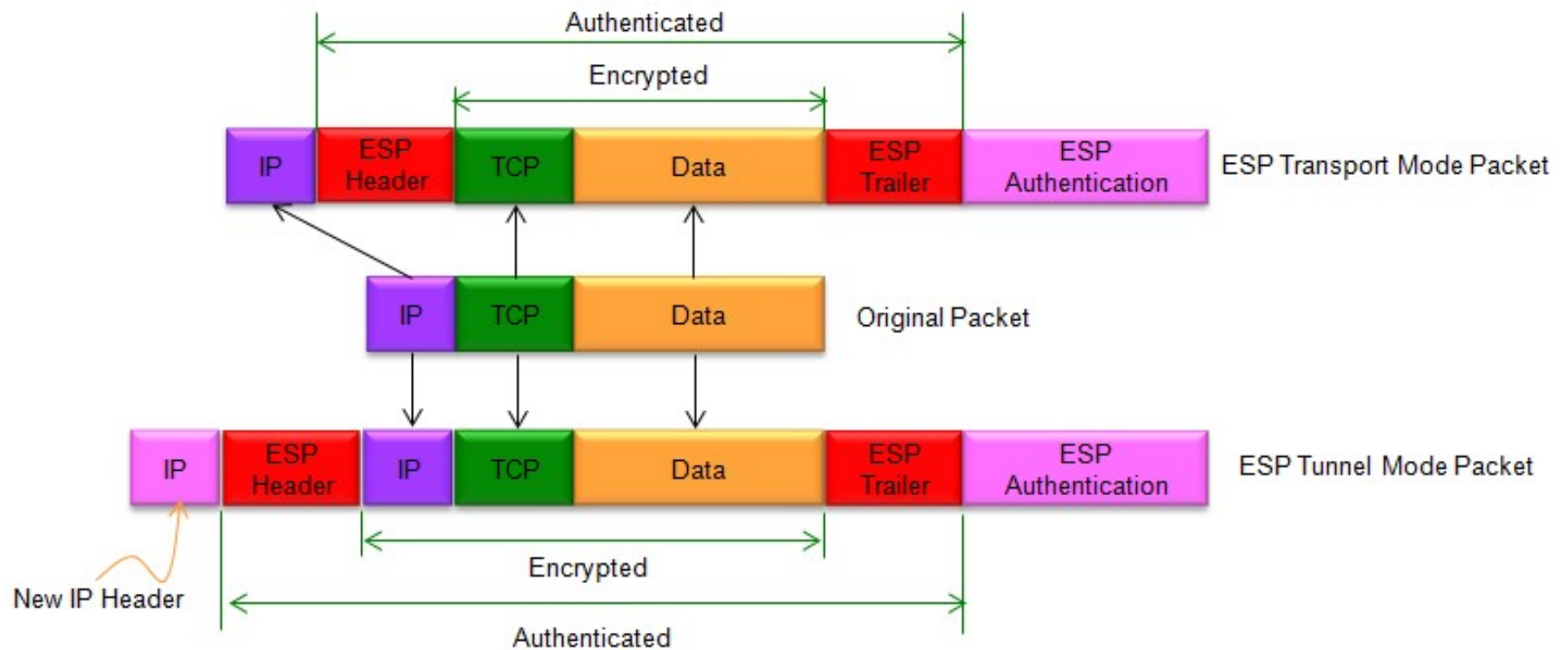
Encryption  
algorithm

# Authentication Header (AH)

Authentication &  
Integrity (No privacy)



# Encapsulating Security Payload (ESP)



Authentication &  
Integrity & Privacy