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.

https://www.servercake.blog
## Site 2 Site vs. Remote Access VPN

<table>
<thead>
<tr>
<th>Remote-Access VPN</th>
<th>Site-to-Site VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Remote-Access VPN, a client software is used on the user’s device.</td>
<td>In Site-to-Site VPN, no client software is needed on the user’s device.</td>
</tr>
<tr>
<td>In Remote-Access VPN, the user needs to initiate the VPN tunnel setup.</td>
<td>In Site-to-Site VPN, the user does not need to initiate the VPN tunnel setup.</td>
</tr>
<tr>
<td>In Remote-Access VPN, the user’s device communicates with the VPN gateway using a VPN tunnel.</td>
<td>In Site-to-Site VPN, the VPN gateway from one LAN communicates with the VPN gateway of another LAN and creates secure VPN tunnel.</td>
</tr>
</tbody>
</table>
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 = ALrXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX1E1I=
Address = 10.0.0.6/24

[Peer]
PublicKey = tLZzlNwXXXXXXXXXXXXXXXXXnE4CWlhnymFk=
PreSharedKey = ycSwXXXXXXXXXXXXXXXXXXXXXDpFH0XUOU=
AllowedIPs = 192.168.19.0/24
Endpoint = 151.69.121.221:1194

## Keep connection alive ##
PersistentKeepalive = 30
VPN activation (client side)

<table>
<thead>
<tr>
<th>Network</th>
<th>Destination</th>
<th>Netmask</th>
<th>Gateway</th>
<th>Interface</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>192.168.179.86</td>
<td>192.168.179.231</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>10.0.0.0</td>
<td>255.255.255.0</td>
<td>On-link</td>
<td>10.0.0.6</td>
<td>261</td>
<td></td>
</tr>
<tr>
<td>10.0.0.6</td>
<td>255.255.255.255</td>
<td>On-link</td>
<td>10.0.0.6</td>
<td>261</td>
<td></td>
</tr>
<tr>
<td>10.0.0.255</td>
<td>255.255.255.255</td>
<td>On-link</td>
<td>10.0.0.6</td>
<td>261</td>
<td></td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>255.0.0.0</td>
<td>On-link</td>
<td>127.0.0.1</td>
<td>331</td>
<td></td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>255.255.255.255</td>
<td>On-link</td>
<td>127.0.0.1</td>
<td>331</td>
<td></td>
</tr>
<tr>
<td>192.168.19.0</td>
<td>255.255.255.0</td>
<td>On-link</td>
<td>10.0.0.6</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>192.168.19.255</td>
<td>255.255.255.255</td>
<td>On-link</td>
<td>10.0.0.6</td>
<td>261</td>
<td></td>
</tr>
<tr>
<td>192.168.179.0</td>
<td>255.255.255.0</td>
<td>On-link</td>
<td>192.168.179.231</td>
<td>311</td>
<td></td>
</tr>
<tr>
<td>192.168.179.231</td>
<td>255.255.255.255</td>
<td>On-link</td>
<td>192.168.179.231</td>
<td>311</td>
<td></td>
</tr>
<tr>
<td>192.168.179.255</td>
<td>255.255.255.255</td>
<td>On-link</td>
<td>192.168.179.231</td>
<td>311</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>240.0.0.0</td>
<td>On-link</td>
<td>127.0.0.1</td>
<td>331</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>240.0.0.0</td>
<td>On-link</td>
<td>192.168.179.231</td>
<td>311</td>
<td></td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>255.255.255.255</td>
<td>On-link</td>
<td>127.0.0.1</td>
<td>331</td>
<td></td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>255.255.255.255</td>
<td>On-link</td>
<td>192.168.179.231</td>
<td>311</td>
<td></td>
</tr>
</tbody>
</table>
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.
    - Negotiates and manages keys.

- **Authentication Header (AH)**
  - Security protocols that protect traffic.

- **Encapsulating Security Payload (ESP)**
  - Authentication algorithm
  - Encryption algorithm
Authentication Header (AH)

Authentication & Integrity (No privacy)

Original IP Header   TCP   Payload

Authenticated – Transport Mode

Original IP Header   AH   TCP   Payload

New IP Header   AH   Original IP Header   TCP   Payload

Authenticated – Tunnel Mode
Encapsulating Security Payload (ESP)

Authenticated & Integrity & Privacy

Original Packet

ESP Transport Mode Packet

ESP Tunnel Mode Packet

New IP Header

Encrypted

Authenticated