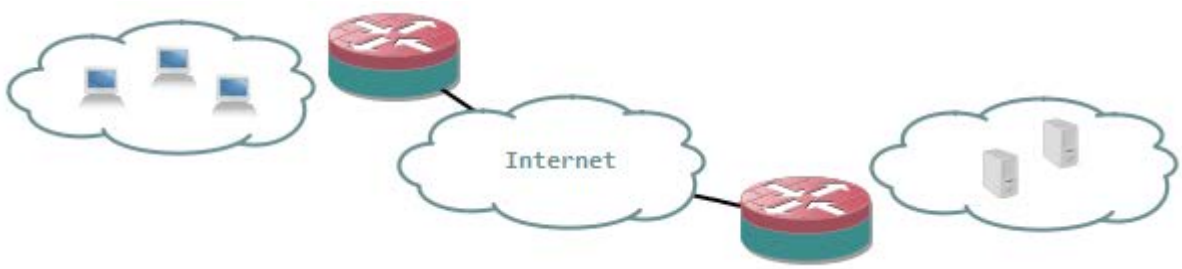
TYPES OF VPN

Since I'm going to talk more about VPNs in the upcoming weeks, I'm going to explain the different types of VPN here. No configuration guides, but an explanation so it's clear what is what.

For those who aren't sure what a VPN is: a **V**irtual Private **N**etwork is an encrypted connection between two or more devices over a public network. Some may argue that it doesn't necessarily has to be encrypted, but when it's not, that's called a tunnel (for me at least). Here's a list of the types:

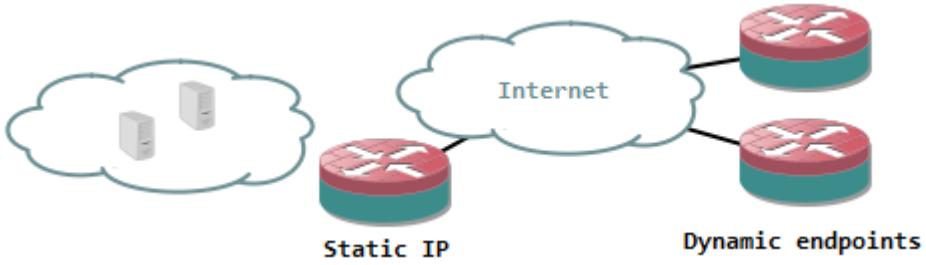


Site-to-site VPN

Often abbreviated to S2SVPN. It's a connection between two sites and encrypts all traffic between two (or multiple) subnets. There are two types of S2SVPN:

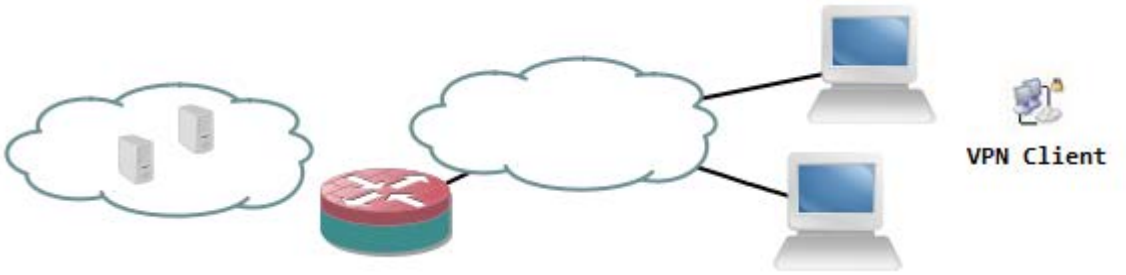
- Policy-based: interesting traffic triggers an ACL and is encrypted and sent to the remote VPN peer.
- Routed: traffic is routed into an encrypted tunnel to the remote VPN peer.

For a detailed explanation and configuration, Jeremy made some excellent posts about this on Packetlife: Part 1 for policy-based and Part 2 for routed.



DMVPN

A dynamic multipoint VPN is not a protocol but more a technique using different protocols. One or more central hub routers are required, but the remote (spoke) routers can have dynamic IPs and more can be added without having to modify the configuration on the hub router(s), or any other spoke routers. The routers use a next-hop resolution protocol, combined with a dynamic routing protocol to discover remote peers and subnets. The VPN itself is a mGRE tunnel (GRE with multiple endpoints) which is encrypted. This way, traffic between spoke routers does not have to go through the hub router but can be sent directly from spoke to spoke.



Client VPN

A client VPN is an encrypted connection from one device towards a VPN router. It makes that one remote device appear as a member of a local subnet behind the VPN router. Traffic is tunneled from the device (usually a computer or laptop of a teleworker) towards the VPN router so that user has access to resources inside the company. It requires client software that needs to be installed and configured.

SSLVPN

This type of VPN works like a client VPN. The difference is that the remote client does not need preconfigured software, but instead the browser acts as VPN software. The browser needs to support active content, which every modern browser supports, either directly or through a plug-in. Traffic is tunneled over SSL (or TLS) to the SSLVPN

router. From a networking perspective, traffic is tunneled over layer 4 instead of layer 3. The benefit is that the remote user does not need to configure anything and can simply log in to a web page to start the tunnel. The drawback that you'll likely need a dedicated device as SSLVPN endpoint because this is not a standard feature.

Source : http://reggle.wordpress.com/2012/03/05/different-types-of-vpn-explained/