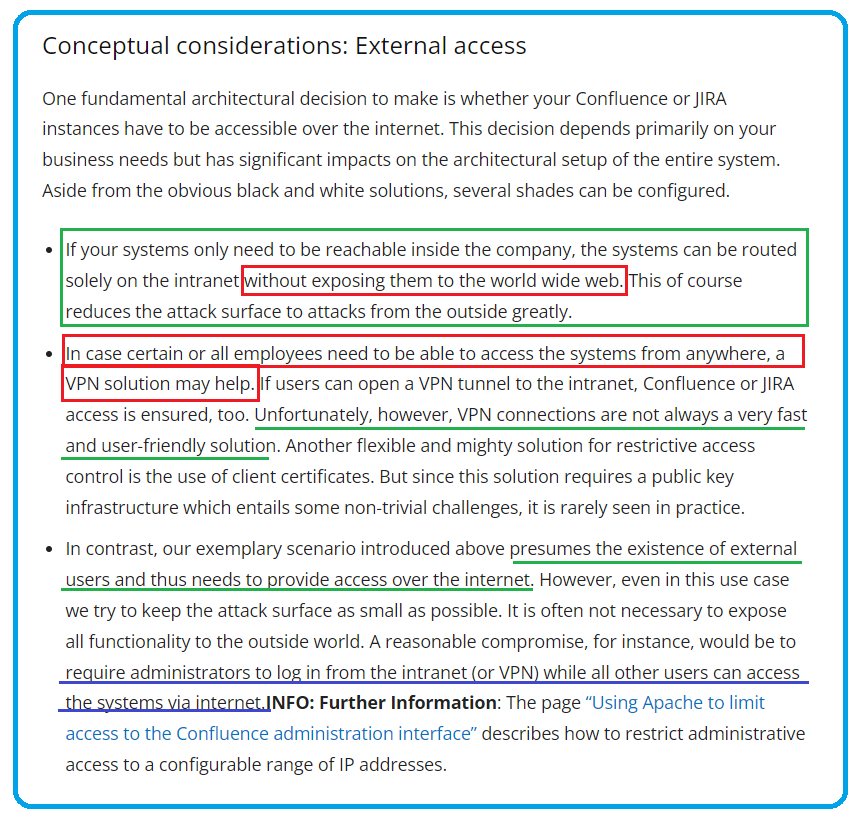
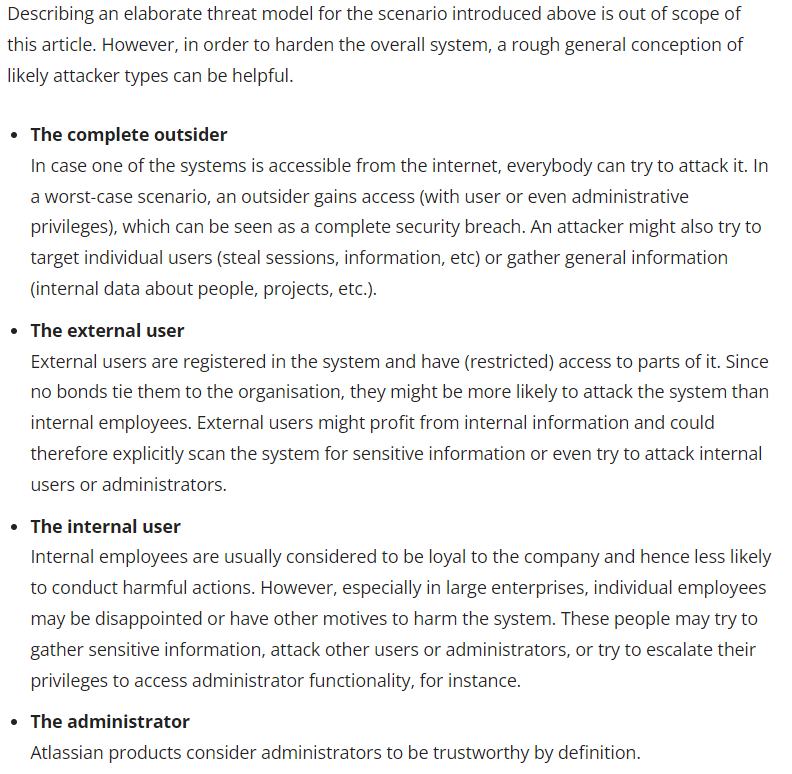
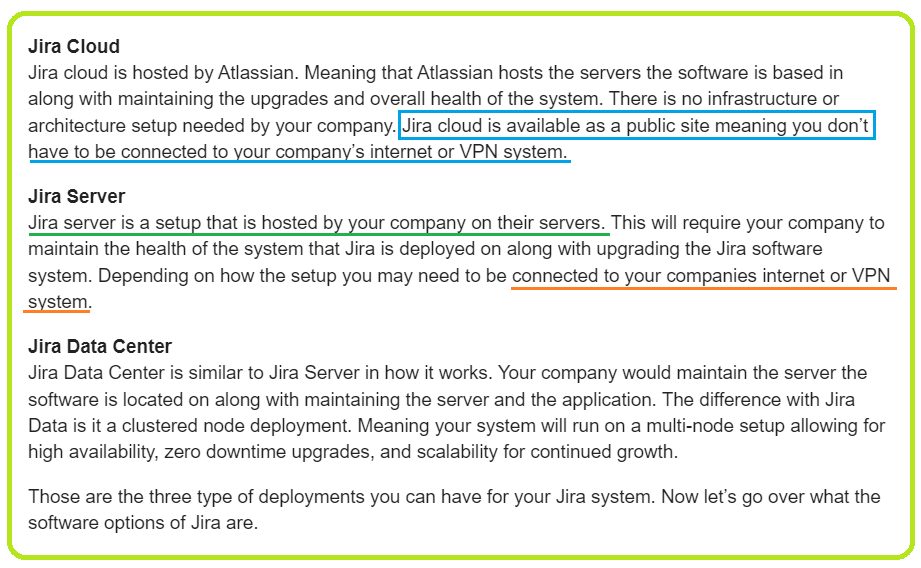
https://docs.oracle.com/en/solutions/connect-onprem-vpn/index.html#GUID-0FC61D33-5141-40FB-8CB4-7E45353BE486

Jira cloud is available as a public site meaning you don’t have to be connected to your company’s internet or VPN system. Your company’s remote access and [mobile access](https://www.microsoft.com/microsoft-365/onedrive/mobile) needs play a role in choosing the right option. Here are some considerations when it comes to accessing your information via the cloud versus on-premises:

### On-premises

If most of your users work in the same office and are rarely mobile—an on-premises server could be a solid choice since you won’t likely need the anywhere access the cloud offers. Also, if you often work with sizable files or videos, you may want to keep them on-premises to keep upload and download times short. (If you use a VPN, keep in mind that unforeseen situations like natural disasters or COVID-19, for example, can suddenly turn office workers into remote workers, which can also overwhelm your VPN system.)

### Cloud

With cloud storage, you have what amounts to a [virtual desktop](https://azure.microsoft.com/services/virtual-desktop/). Workers can access anything they do in the office via a cloud server, as long as they have an internet connection. This convenience makes the cloud a great choice for employees who will be using it frequently from home or while they’re on the move, without the need for a VPN.

Cloud servers are also perfect for running applications that need to be always up and available**.**In addition, the cloud allows for easy [file sharing](https://www.microsoft.com/microsoft-365/onedrive/online-cloud-storage), real-time collaboration and better version control. Lastly, some cloud storage providers offer differential sync, which dramatically reduces the upload time and bandwidth used when making changes to huge files.

What is a VPN and how does it work?

A **virtual private network (VPN)** is a series of virtual connections routed over the internet which **encrypts your data** as it travels back and forth between your **client machine and the internet resources** you're using, such as web servers. Many internet protocols have built-in encryption, such as [HTTPS](https://en.wikipedia.org/wiki/HTTPS), [SSH](https://cybersecurity.att.com/blogs/security-essentials/explain-how-ssh-works-to-me), [NNTPS](https://en.wikipedia.org/wiki/Network_News_Transfer_Protocol), and [LDAPS](https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx). So assuming that everything involved is working properly, if you use those ports over a VPN connection, your data is encrypted at least twice!

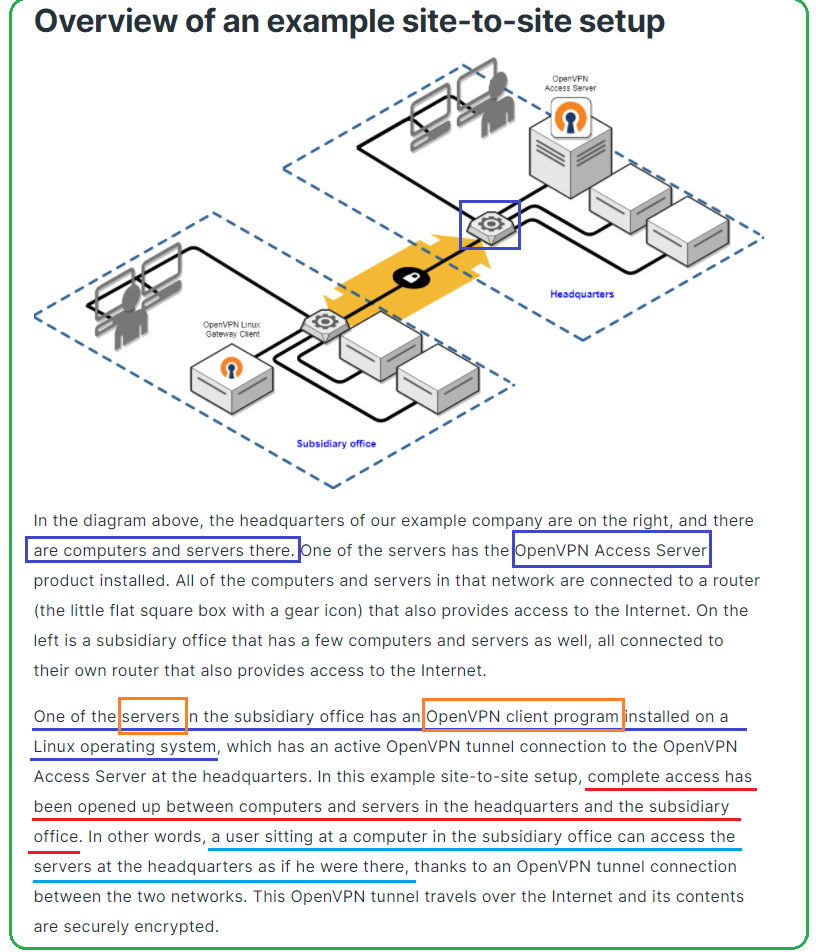
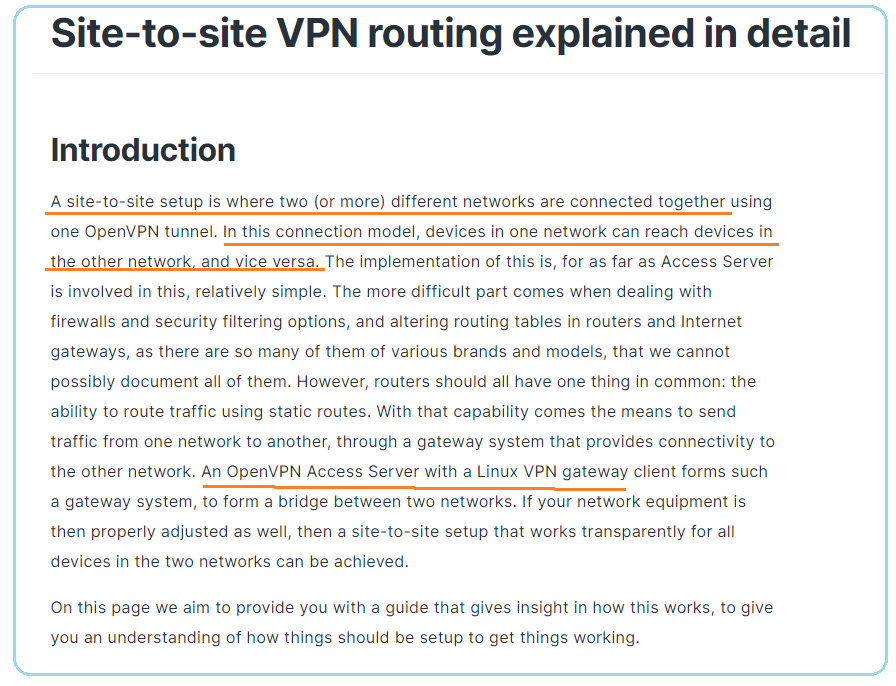
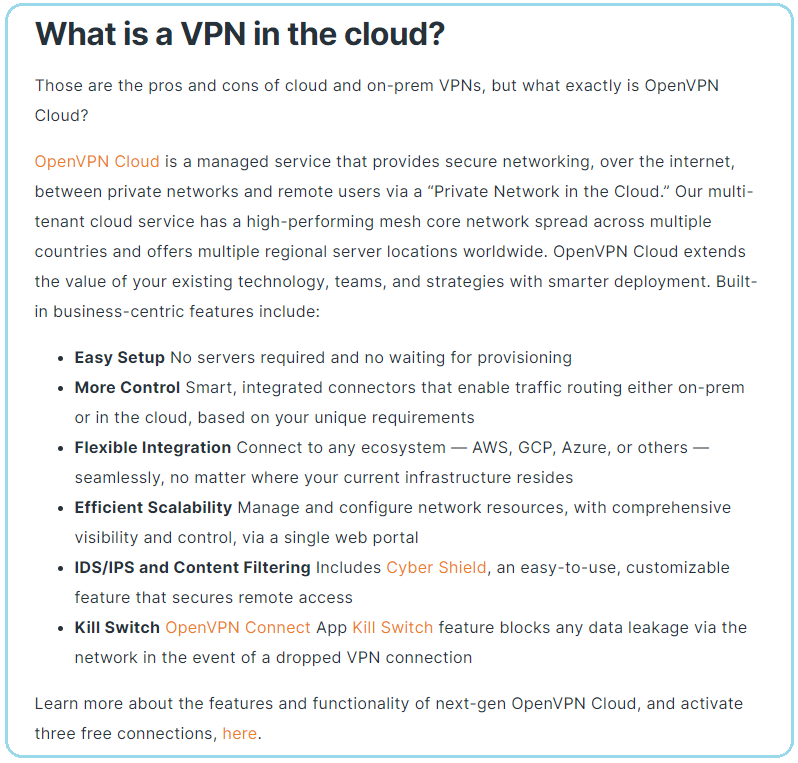
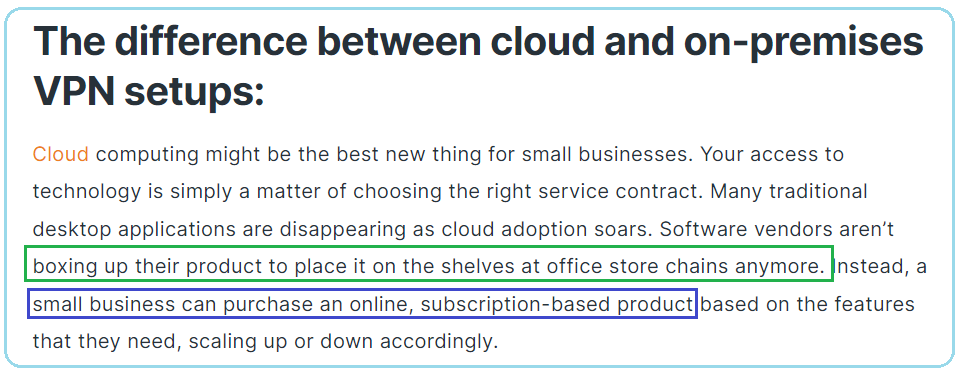
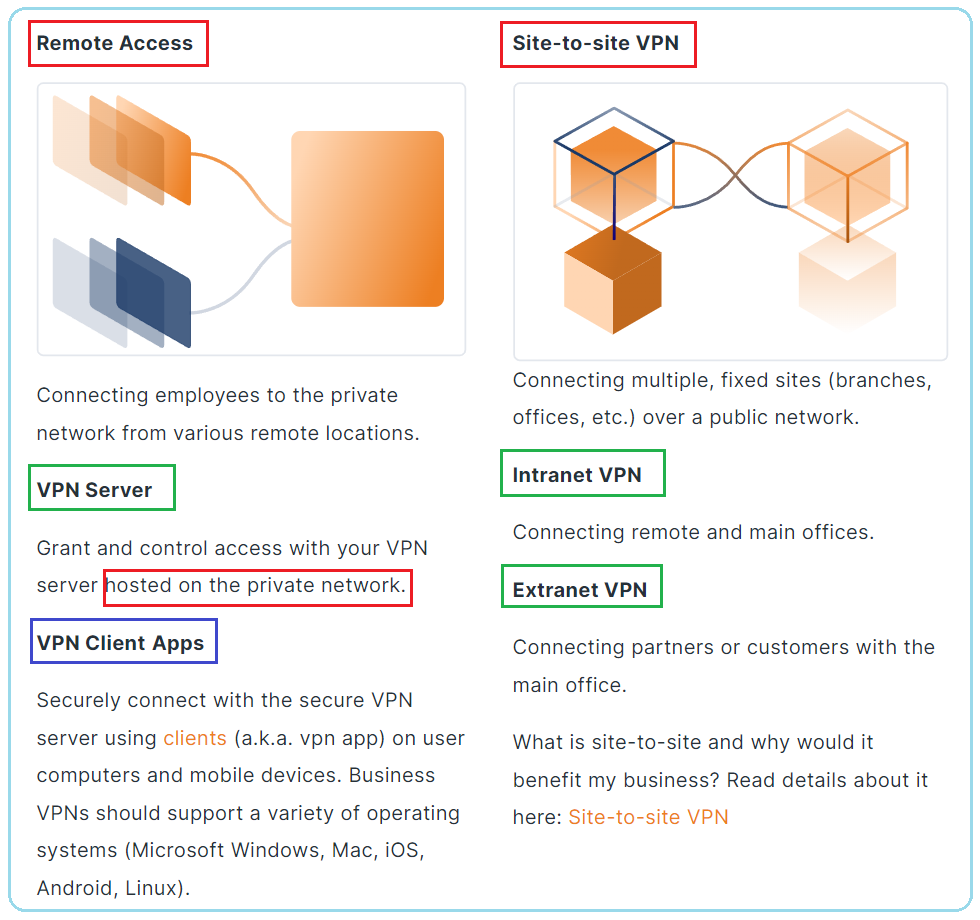
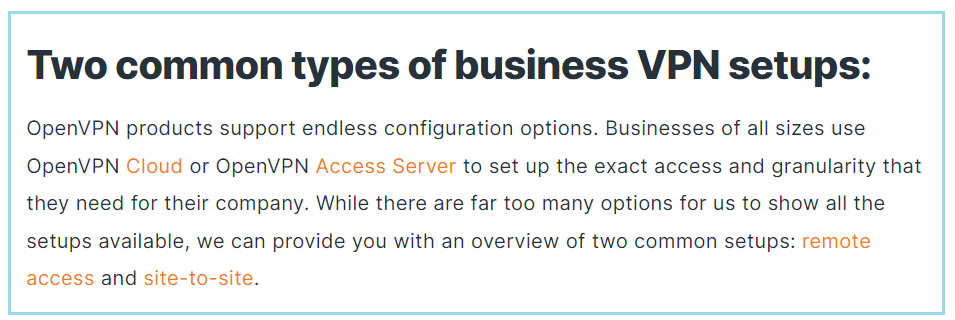
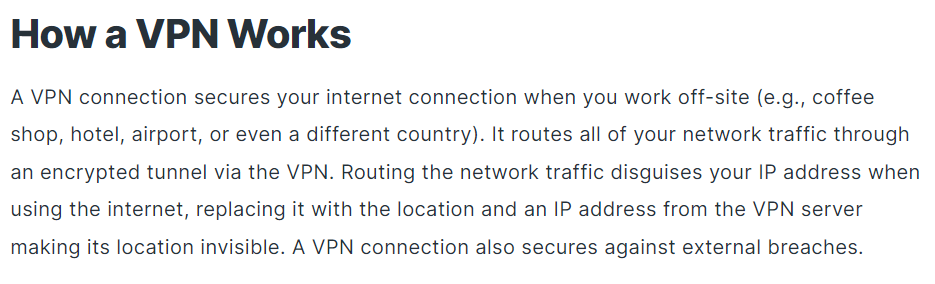
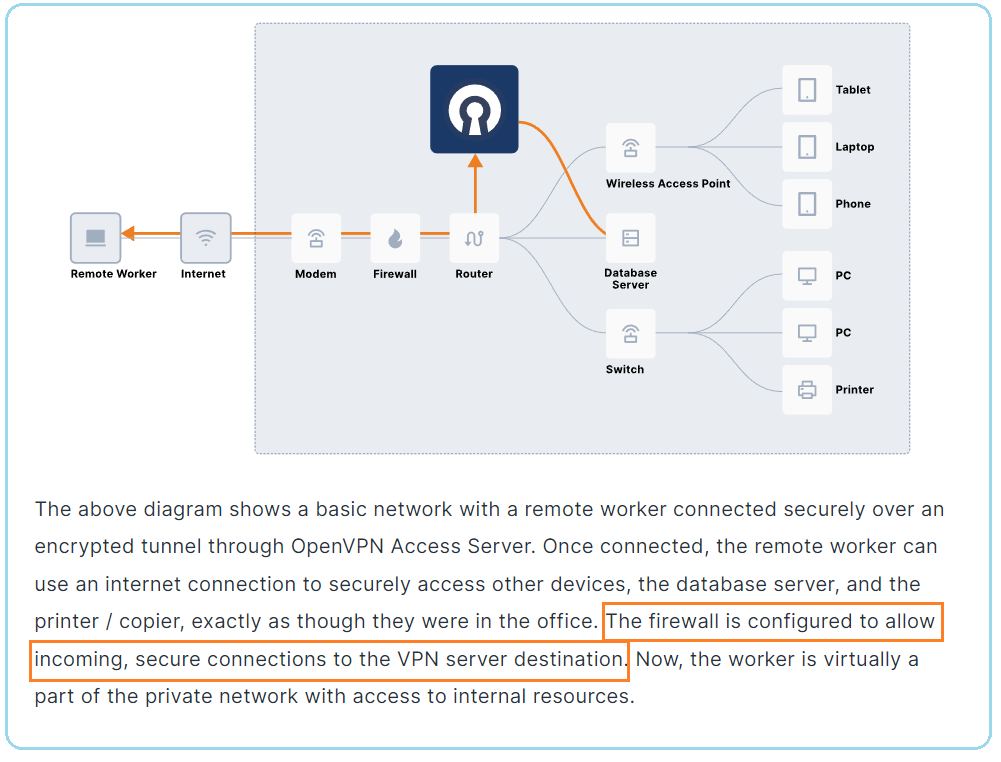
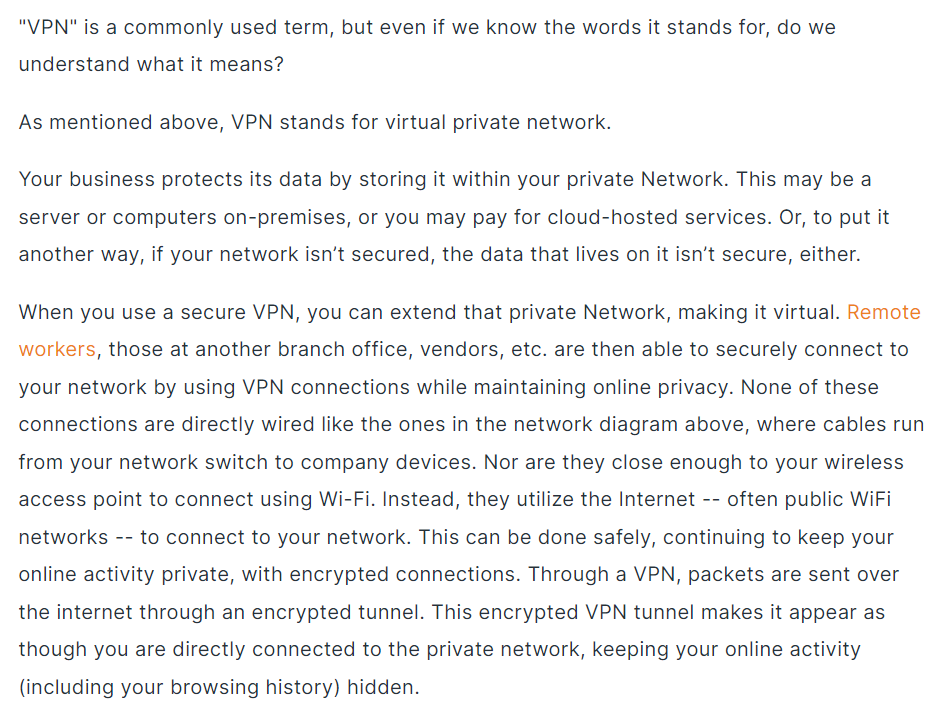
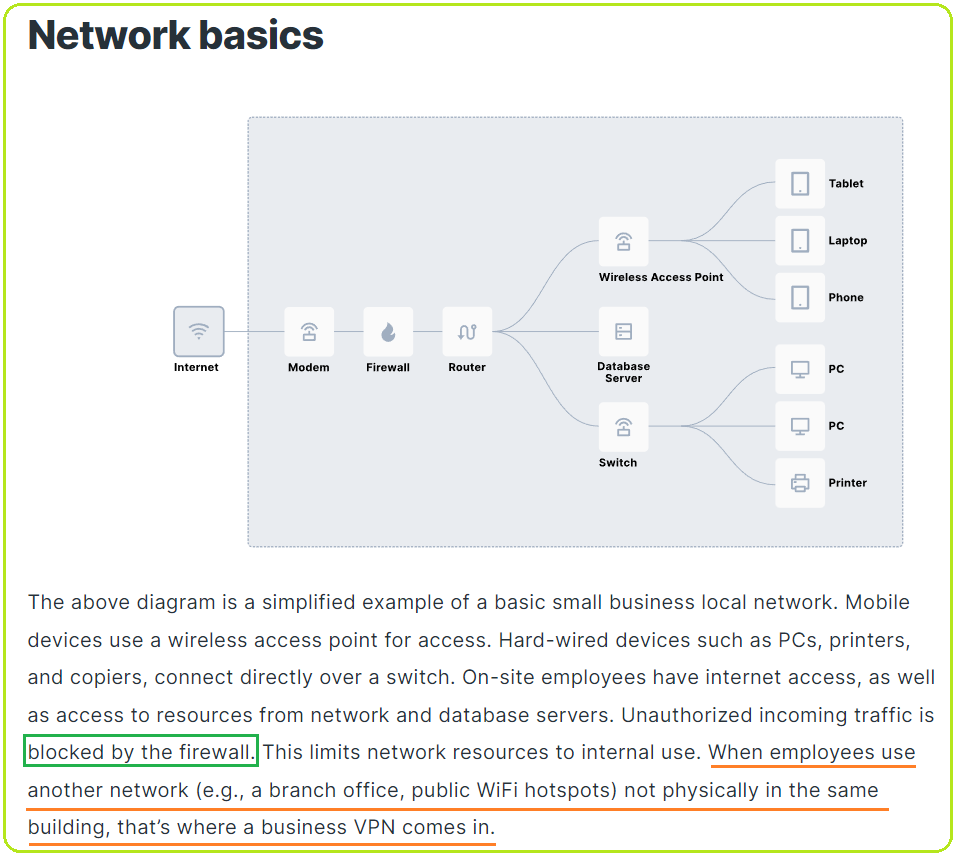
PCs, smartphones, tablets, dedicated servers, and even some IoT devices can be **endpoints for a VPN connection**. Most of the time your client will need to use a VPN connection application. Some routers also have built-in VPN clients. Unlike proxy networks such as Tor, VPNs shouldn't noticeably slow down your internet traffic under usual circumstances. But some VPNs are faster than others, and one of the most important factors is how many VPN clients are using a VPN server at any given time.

A VPN connection usually works like this. Data is transmitted from your client machine to a point in your VPN network. The VPN point encrypts your data and sends it through the internet. Another point in your VPN network decrypts your data and sends it to the appropriate internet resource, such as a web server, an email server, or your company's intranet. Then the internet resource sends data back to a point in your VPN network, where it gets encrypted. That encrypted data is sent through the internet to another point in your VPN network, which decrypts the data and sends it back to your client machine. Easy peasy!

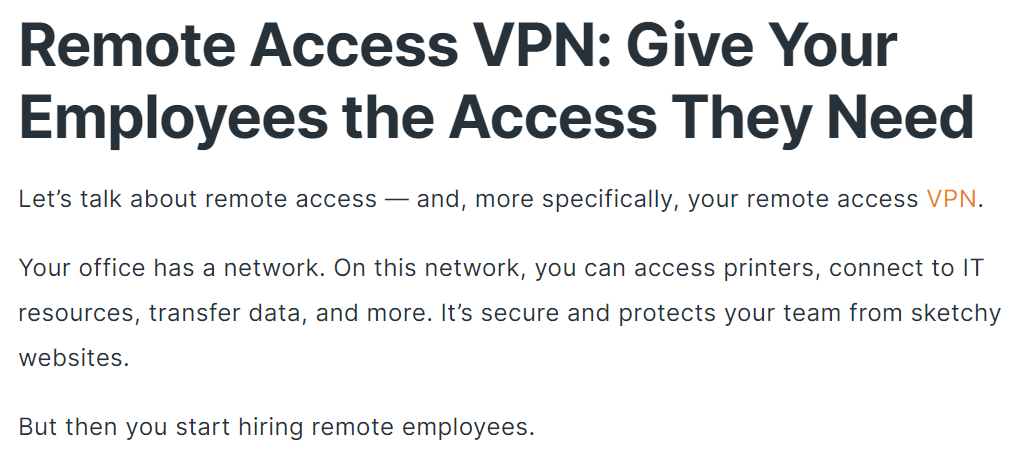
## Types of VPN technologies

Different VPNs can use different encryption standards and technologies. Here's a quick list of some of the technologies that a VPN may use:

* **Point-to-Point Tunneling Protocol: PPTP** has been around since the mid 1990s, and it's still frequently used. PPTP in and of itself doesn't do encryption. It tunnels data packets and then uses the GRE protocol for encapsulation. If you're considering a VPN service which uses PPTP, you should keep in mind that security experts such as Bruce Schneier have found the protocol, [especially Microsoft's implementation of it](https://www.schneier.com/academic/pptp/faq.html), to be quite insecure.
* **IPSec**: You should consider IPSec to be a better alternative to PPTP. IPSec is actually a suite of different protocols and technologies. Packet encapsulation is done through the ESP protocol, and AES-GCM, AES-CBC, 3DES-CBC, or HMAC-SHA1/SHA2 may be used for encryption.
* Layer 2 Tunneling Protocol: L2TP can be used for tunneling with IPSec for added security.
* [**Secure Shell**, otherwise known as SSH](https://www.alienvault.com/blogs/security-essentials/explain-how-ssh-works-to-me) can be used to handle both the tunneling and encryption in a VPN network.

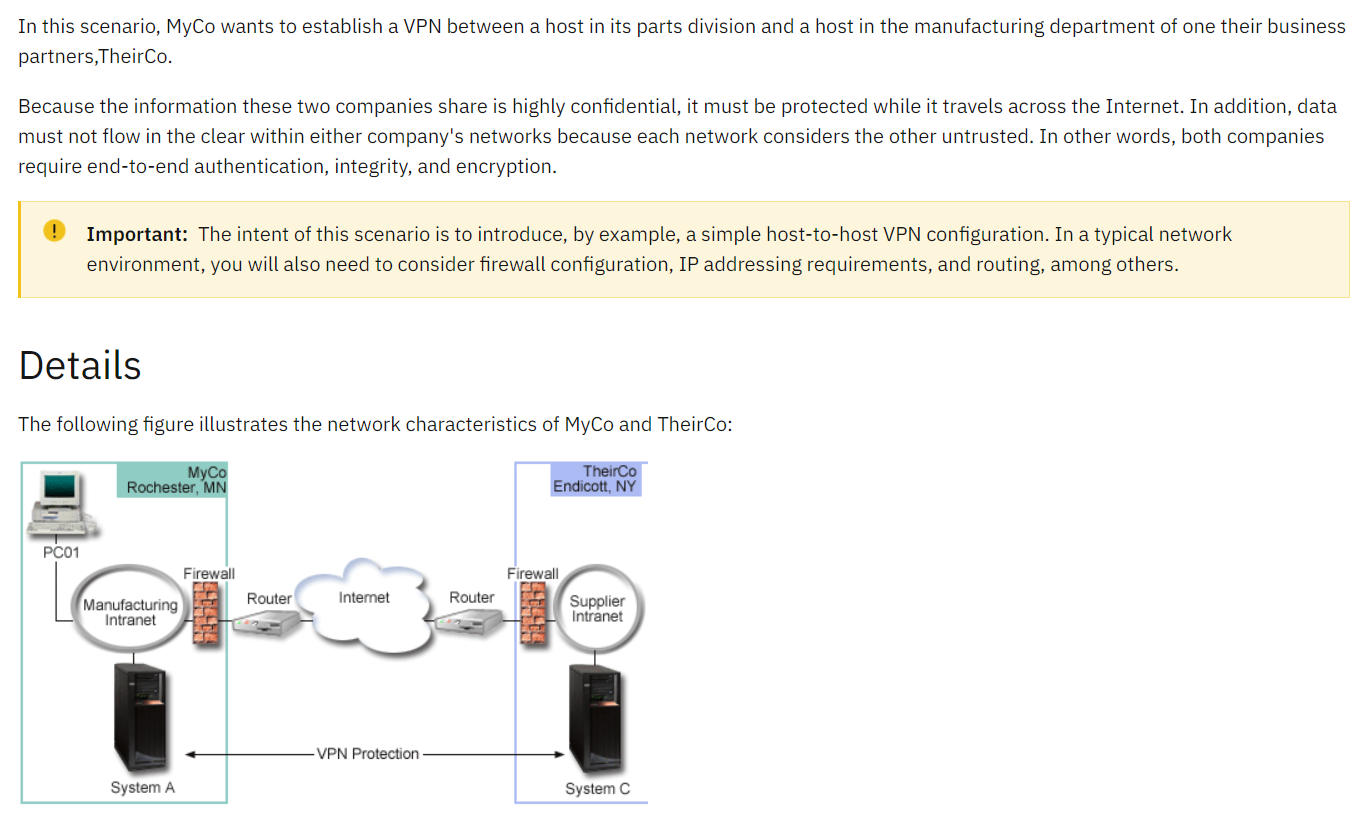
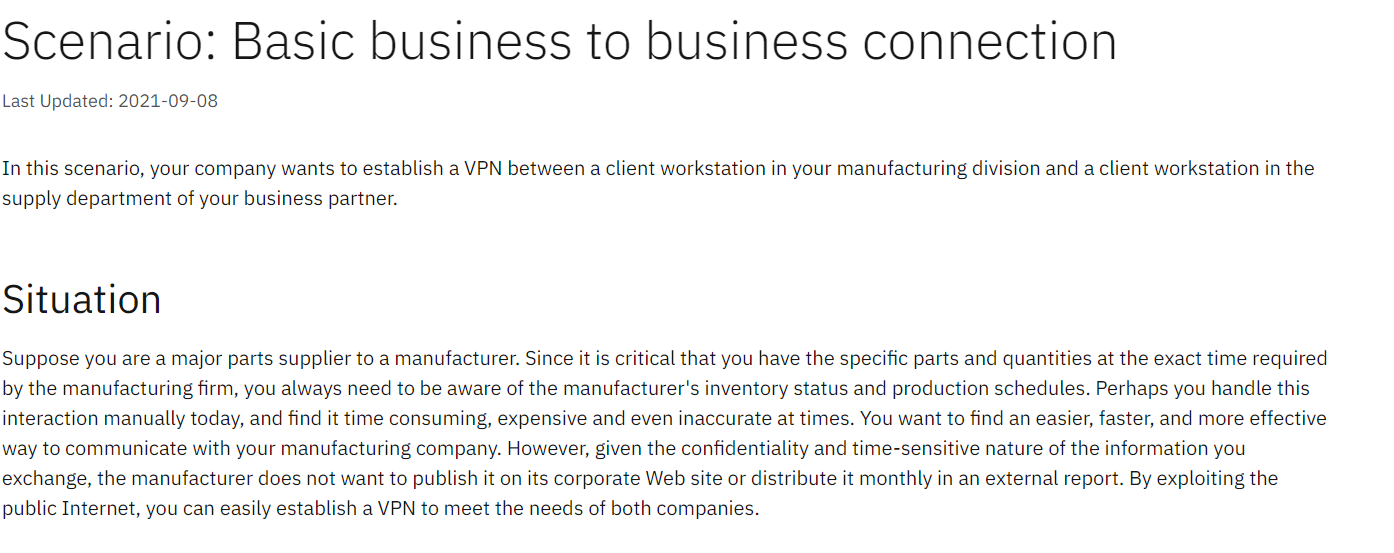


<https://openvpn.net/vpn-server-resources/site-to-site-routing-explained-in-detail/>



<https://www.ibm.com/docs/en/i/7.4?topic=scenarios-scenario-basic-business-business-connection>

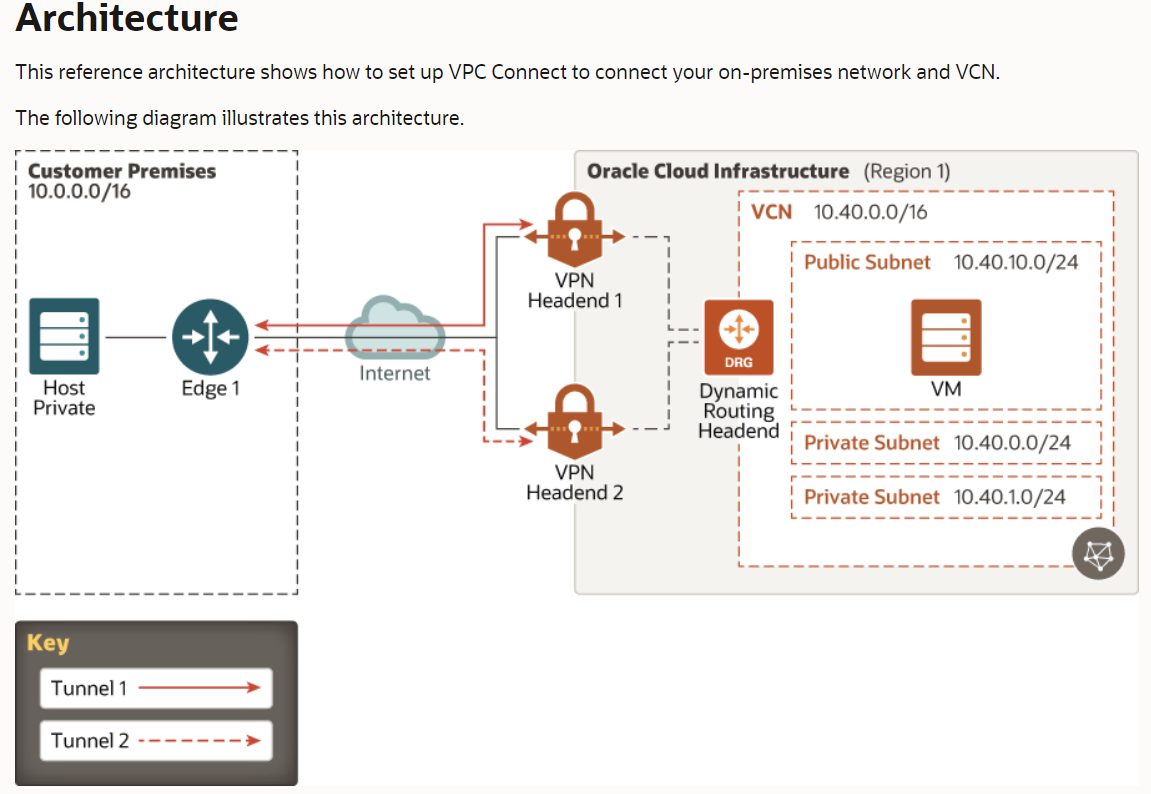
<https://www.scalefactory.com/blog/2020/12/14/how-to-set-up-a-site-to-site-vpn-connection/>



# Connect your on-premises network using VPN

<https://docs.oracle.com/en/solutions/connect-onprem-vpn/index.html#GUID-D96D1542-CACC-4294-A870-E0BD4A6730D2>

<https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/overviewIPsec.htm>



A firewall allows you to establish certain rules to identify the traffic that should be allowed in or out of your private network. Depending on the type of firewall implemented, you can **restrict access to only certain IP addresses and domain names**, or you can **block certain types of traffic by blocking the**[**TCP/IP**](https://www.lifewire.com/transmission-control-protocol-and-internet-protocol-816255)**ports** they use.

<https://www.softwaretestinghelp.com/firewall-security/>

### Firewall

Firewalls are important because they protect you from viruses and other security issues based on the security parameters you set. This security measure controls incoming and outgoing traffic on your computer. You can use firewalls to **allow or block traffic on specific websites** according to the state, protocol, or port. Many firewalls also feature antivirus software that provides an additional layer of security for the computers on your private [business network](https://businessupside.com/2021/03/20/make-a-social-network-app-and-rule-the-world/). You can place your firewall before or after your router to safeguard against external threats. Because of the nature of firewalls, the icon to represent a firewall is often a brick wall.

### Routers

Routers are devices that transfer data between networks. This device enables different networks to communicate. You can communicate between your private business network and the internet, your server and private network, or different networks that are connected to each other. If you are **connecting your router to the internet**, make a line from the cloud-like symbol (your internet connection) to the router symbol. The standard symbol for a router is a single circle with four arrows revolving around the circle. The left and right arrows need to be pointing inward, while the arrow on the top points up and the bottom arrow points down. If you plan on using a wireless router, make sure you add two antennas at the top of the circle

### VPN

The [virtual private network](https://www.forbes.com/sites/tjmccue/2019/06/20/benefits-of-a-vpn/?sh=3bb8b51e2466) (VPN) is **a necessity for all private networks that are connected to the internet**. The VPN filters internet traffic using an external proxy server, making tracing the IP address of the devices on your private network nearly impossible. The VPN symbol is represented by a padlock. Check the review portal [Top50vpn.com](https://www.top50vpn.com/) for more insights about VPN and its benefits.

### Server

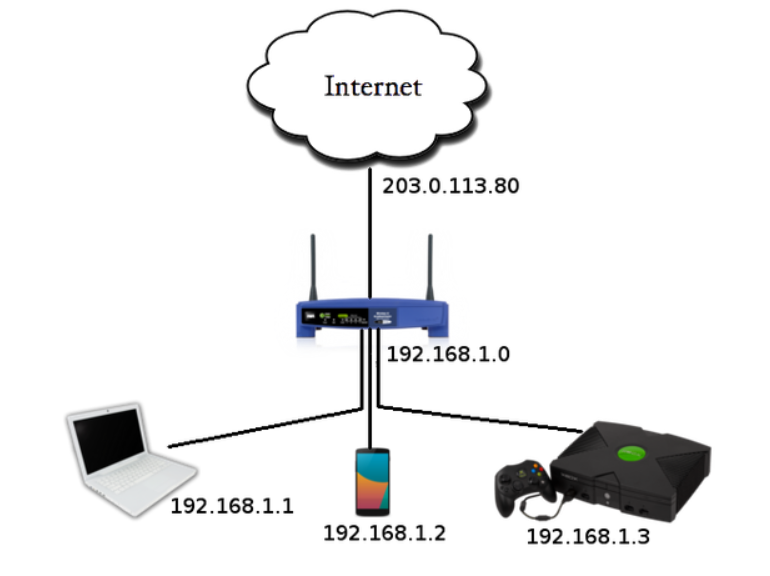
All servers you plan on using for your [business](https://businessupside.com/2021/04/09/small-business-ideas-that-you-can-start-with-a-small-budget/) need to be connected to your router. Many networks have one or multiple servers that feature centralized programs and data that all computers that are connected to the network can use.

### Hubs

You also need to know about switches and hubs for your private business network. While **hubs and switches** enable the devices that are connected to your network to communicate, **your router enables different networks** to communicate. A **hub** will evenly distribute your network’s total bandwidth between all the devices on your network. **Switches** will allocate your network’s total bandwidth to the devices on your network that needs it the most. The universal symbol for switches and hubs is a rectangle with arrows at both ends and a pair of lines that cross in the middle.

Every home network is a “private network” that is connected to the internet.  
Private network being in quotes because it is no longer 100% private once it is connected to another network.

Every device must have an IP address to communicate on the network.  
There is far far too many devices to give every device an internet route-able IP address. **So you get one IP from your ISP for your whole house (or company),** making numbers up lets say 63.27.12.152. Then you router creates a local “private” network and gives each device an IP address for the private network (this is the 192.168.x.y address. When any device on the local network wants to connect to say access a website on the internet, it uses the router as a middle man and the router communicates with the webserver using its 63.27.12.152 IP address.

The way things get negotiated between the wide internet and your home is something called [**Network address translation**](https://en.wikipedia.org/wiki/Network_address_translation)**, or NAT**. In your router, there is software which keeps track of the translations so that every device can communicate. So your router has one foot in your private network and another on the Internet.

Your home network is a [Private network](https://en.wikipedia.org/wiki/Private_network) and the IP Addresses are usually in the 192.168.0.0 to 192.168.255.255 range (that is for the most common protocol, known as IPv4). That means that you can have over 65 thousand devices on your private network! Your router will have two IP addresses - one on your side of the network, one for the internet, as in this diagram:

When you connect to your PC by using a Remote Desktop client, you're creating a peer-to-peer connection. This means you need direct access to the PC (sometimes called "the host"). If you need to connect to your PC from outside of the network your PC is running on, you need to enable that access. You have a couple of options: **use port forwarding or set up a VPN**.

## What’s Dynamic DNS And Why Would I Want It?

**RELATED:** [**What Is DNS, and Should I Use Another DNS Server?**](https://www.howtogeek.com/122845/htg-explains-what-is-dns/)

Before dive into the tutorial and before we even start talking about what dynamic DNS (DDNS) is, let’s start with the basics–[what DNS even is](https://www.howtogeek.com/122845/htg-explains-what-is-dns/). DNS, or Domain Name System, is the magic that makes the internet user friendly, and the greatest thing since sliced bread.

Every internet-accessible resource–web pages, FTP sites, you name it–has an IP address that serves as the resource’s network address on the internet. These addresses are numeric, in the format 123.123.123.123, and are not particularly easy to remember. Remember the last time you went to 66.220.158.68 to check up on pictures of your niece? No? Of course you don’t, because you typed facebook.com into your web browser instead of 66.220.158.68. A DNS server resolved your human-friendly request of facebook.com into a machine-friendly address that sent you, probably in a hundredth of a second or less, to Facebook.

Wouldn’t it be great if you could set up the same trick for your home network? This is where Dynamic DNS (DDNS) comes into play. **It’s easy to for big companies to set up domain names like Facebook.com because the address of their web server is static (once they have the IP address it doesn’t change)**. Your home IP address is different though. People with residential connections get a dynamically assigned IP address. Your ISP has a big pool of addresses and they share them with everyone on an as-needed-basis. This makes it pretty difficult to pull the same trick that is so easy for the likes of Coca-Cola because the address you have today isn’t the address you might have next week. Thankfully DDNS providers make it dead simple to assign a memorable name to your home IP address because they update automatically as your IP address changes over time.

It does not alter your home network settings in anyway so whatever worked (or didn’t work) before you set up the DDNS system will keep working (or not working) with the new DDNS address. If you used to connect to your home music server while you were at work by visiting **XXX.XXX.XXX.XXX:5900** (your home IP address, port 5900) you can now connect to it at **yournewDDNSaddress.com:5900**.

## What Is Port Forwarding?

There are plenty of projects we’ve covered that use your computer as a server for other devices. When you’re inside of your network, most things will work fine. But some apps, if you want to access them when you’re outside your network, make things significantly hairier. Let’s start by taking a look at why that is.

### How Your Router Handles Requests and Uses Ports

Here’s a map of a simple home network. The cloud icon represents the greater internet and your public, or forward-facing, Internet Protocol (IP) address. **This IP address** represents your *entire household from the outside world*–like a street address, in a way.

The red address 192.1.168.1 is the router address within your network. The additional addresses all belong to the computers seen at the bottom of the image. If your **public IP address is like a street address**, think of the internal IP addresses like apartment numbers for that street address.

The diagram raises an interesting question which you may not have thought about before. How does all the information from the internet get to the right device inside the network? If you visit howtogeek.com on your laptop how does it end up on your laptop and not your son’s desktop if the public-facing IP address is the same for all devices?

This is thanks to a wonderful bit of routing magic known as a **Network Address Translation (NAT)**. This function occurs at the router level where the NAT acts like a traffic cop, directing the flow of network traffic through the router so that a single public IP address can be shared among all the devices behind the router. Because of the NAT, everyone in your household can request web sites and other internet content simultaneously and it will all be delivered to the right device.

So where do ports come into this process? Ports are an old but useful holdover from the early days of network computing. Back in the day, when computers could only run one application at a time, all you had to do was point one computer at another computer on the network to connect them as they would be running the same application. Once computers became sophisticated to run multiple applications, early computer scientists had to wrestle with the issue of ensuring applications connected to the right applications. Thus, ports were born.

Some ports have specific applications which are standards throughout the computing industry. When you fetch a web page, for example, it uses port 80. The receiving computer’s software knows that port 80 is used for serving http documents, so it listens there and responds accordingly. If you send an http request over a different port—say, 143—the web server won’t recognize it because it’s not listening there (although something else might be, like an IMAP email server which traditionally uses that port).

Other ports don’t have pre-assigned uses, and you can use them for whatever you want. To avoid interfering with other standard-abiding applications, it’s best to use larger numbers for these alternate configurations. Plex Media Server uses port 32400, for example, and Minecraft servers use 25565—both numbers that fall into this “fair game” territory.

