robustel

A Practical Guide to 3G/4G (IoT) Router Security

Introduction

"IoT Security" is a broad phrase. So broad as to arguably be meaningless in its own right. So, to open, we need to define the scope and purpose of this article to position it clearly in the IoT hierarchy.

This article introduces some of the security concepts associated with deploying cellular (3G/4G) routers + Gateways such as those sold by Robustel and other manufacturers around the world.

The architecture of such deployments typically involves a router, a SIM card and a connected device such as a PLC, IP Camera, BMS Controller, media player or other similar device at the edge, using publicly available cellular networks to move data from the edge to the cloud.

Data and the infrastructure itself can be vulnerable to malicious behaviour and this article takes a practical view on the general and Robustel-specific solutions to these "IoT Security" challenges.

Section 1 – Choice of SIM Card

Ironically, the most critical security consideration in a router deployment is the SIM card.

The SIM card is directly responsible for the IP Addressing schema associated with the WAN interface of the router.

One of the most stark examples of this concept is when installers use Public IP addressable SIM cards (still available from some MNOs / MVNOs around the world). With a Public IP address on the SIM anyone on the public internet can see the "front door" to your router. With port forwarding enabled on the router, not only can the router itself be directly accessed but the devices connected on the LAN side of the router also present themselves for all to see!

The more savvy network architect may argue that with remote access turned off (HTTP/HTTPS/SSH blocked on router and attached devices) & a less well known port number used for the port forwarding, then the security risk is mitigated and to an extent this is true.

However, brute force attempts towards the Public IP of the router have to cross the 3G/4G network for them to be dropped by the firewall of the WAN interface of the router. This means the data has traversed the operator's network in one direction. This means all such (unsolicited) data is chargeable by the person that signed the SIM contract. Concerted attacks could cost you GBs of data per month. Multiply this by a large estate of routers and multiply again by an expensive SIM tariff and you have a commercial disaster even if you mitigated a security disaster.

Tip #1 – Don't use Public IP SIM cards

The first part of your security journey is simple – make sure your SIM has a private IP address, not a public one.

Some specialist SIM providers will offer a static or dynamic private IP address. So long as that provider has their house in order and have suitable security in place on their own infrastructure then fixed or dynamic private IP is moot – they both offer an acceptable level of security.

Figure 1.1 shows a simplified view of how a "Thing" communicates with the cloud – or more specifically – an application server on the internet. The important thing to note here is the "APN".

An APN is a fairly abstract concept, not discussed very openly by network operators but is a route that your IoT data will take every day. To that end, it is ironic how little is known about this "giant router in the sky" and how pivotal it is to the success of your application. In simple terms, the APN is gate-keeper to the internet and to other networks reachable via the internet. It is ultimately responsible for your IP address allocation whether fixed or static.

So, when you use a 3G/4G network, your data has a major performance and security dependency on the chosen operator and so the quality of their security becomes the quality of your security.

Tip #2 – Ask your SIM provider about 'penetration tests' on their network and for similar reassurances that your data is being well protected. Ask for a network diagram of their network if you want to understand it more fully

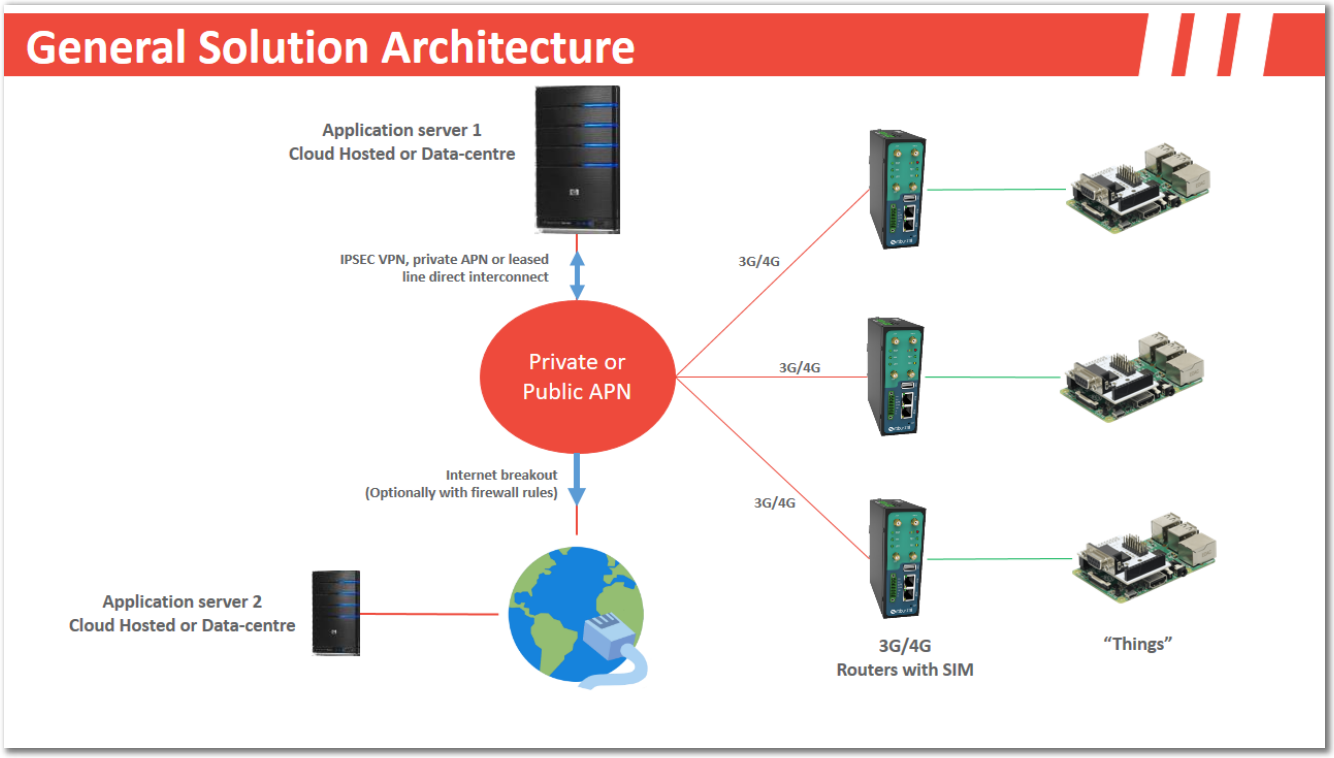

Figure 1.1 – Typical 3G/4G Router solution architecture showing location of APN

Over the air encryption of 3G and 4G networks is a topic at the heart of a detailed security analysis of cellular communications. However, this article makes an assumption that the current encryption standards are adequate for the purposes of most IoT applications.

If the reader has concerns about OTA encryption then they have two options:

1 – Dig deep into the specifications for the various RANs (Radio Access Networks) and/or consult a security specialist on the subject to see what crypto standards have been cracked and how it might impact you.

2 – Implement end-to-end encryption in your application meaning a cracked encryption key will only reveal another layer of encrypted traffic. A common way to do this on a 3G/4G router is to use one of the VPN services directly available on the router itself. VPNs are discussed later in Section 4.

Physical security of the SIM itself can be an important consideration too. A stolen SIM could result in an IP network breach (unlikely) but more likely poses a threat of data or voice traffic charges whilst the SIM is lost but not barred.

Tip #3 – Ask your SIM provider if they can lock down the SIM by 'TAC' code or similar meaning the SIM will not get network access outside of the intended hardware

Section 2 – Physical Security

With the right choice of SIM, attacks from the WAN side of the router are much less likely so we turn our attention to physical security – generically, what could someone with physical access do to the device and how do we mitigate such threats.

Disable Ethernet Ports and DHCP on Ethernet Ports

The Ethernet port is an important medium for being attacked. When it is not needed to be used, it can be turned off through system settings to avoid malicious access by connecting a PC or laptop. If at least one Ethernet port needs to be used, then it is a good idea to switch off DHCP on the LAN side of the router so connected devices do not automatically get an IP address in the right range to obtain internet access. A logical extension of this might be to choose a small and obscure subnet for the LAN side of the router so the chance of a random correct guess by a passer-by is very improbable.

USB Interface Key Validation

Many 3G/4G routers offer a very simple mechanism for configuration update via a USB key.

The USB interface is also a target of the physical media being attacked. Each Robustel router has an independent key generated by the OS and request the Key for authentication whenever there has USB disk inserted. The USB disk must store this key to update the files. In this way the USB port can serve a single function (automatic configuration update) in a secure fashion.

Disable Console Access

Modern routers and much of the equipment connected to them present a user interface to the outside world via web GUI (HTTP/HTTPS), SSH or similar. Disabling such consoles is a good idea unless required and if required, make sure that only permitted users can reach the relevant IP subnet on which console access is available.

Tip #4 ***– a useful trick to alert system administrators to LAN-side issues is to configure an alert, either in the cloud platform (see rcms-cloud.robustel.net) or directly from the router (SMS/Email) that an Ethernet cable has been unplugged – whether it is malicious or not can be quickly determined thereafter.***

Section 3 – WiFi Security

The most effective way to secure WiFi is not to use it. If you do need to use it, make sure WPA security is used as a minimum.

WPA-Enterprise adds additional Radius authentication but can be complex to configure.

A more simple (but less scalable) way to manage individual WiFi clients is to use an Access Control List whereby only white-listed MAC addresses are allowed to join the relevant SSID (wireless network).

Tip #5 ***– Disabling 'SSID Broadcast' in the router AP can be a smart way to enhance security. This means the network name will not be visible to passers-by that perform a network scan but wifi access will still be accessible to those with the right configuration and password.***

Section 4 – VPN Options

There are many ways in which VPNs such as OpenVPN, PPTP, L2TP and IPSEC can be used. Key considerations are exactly where the VPN endpoints are and in who's jurisdiction do they exist? As highlighted in Section 1 it is essential to think of router connections in the context of the SIM provider's network to understand the complete picture. Below we highlight the most commonly used VPN Architectures.

a) End to End VPN

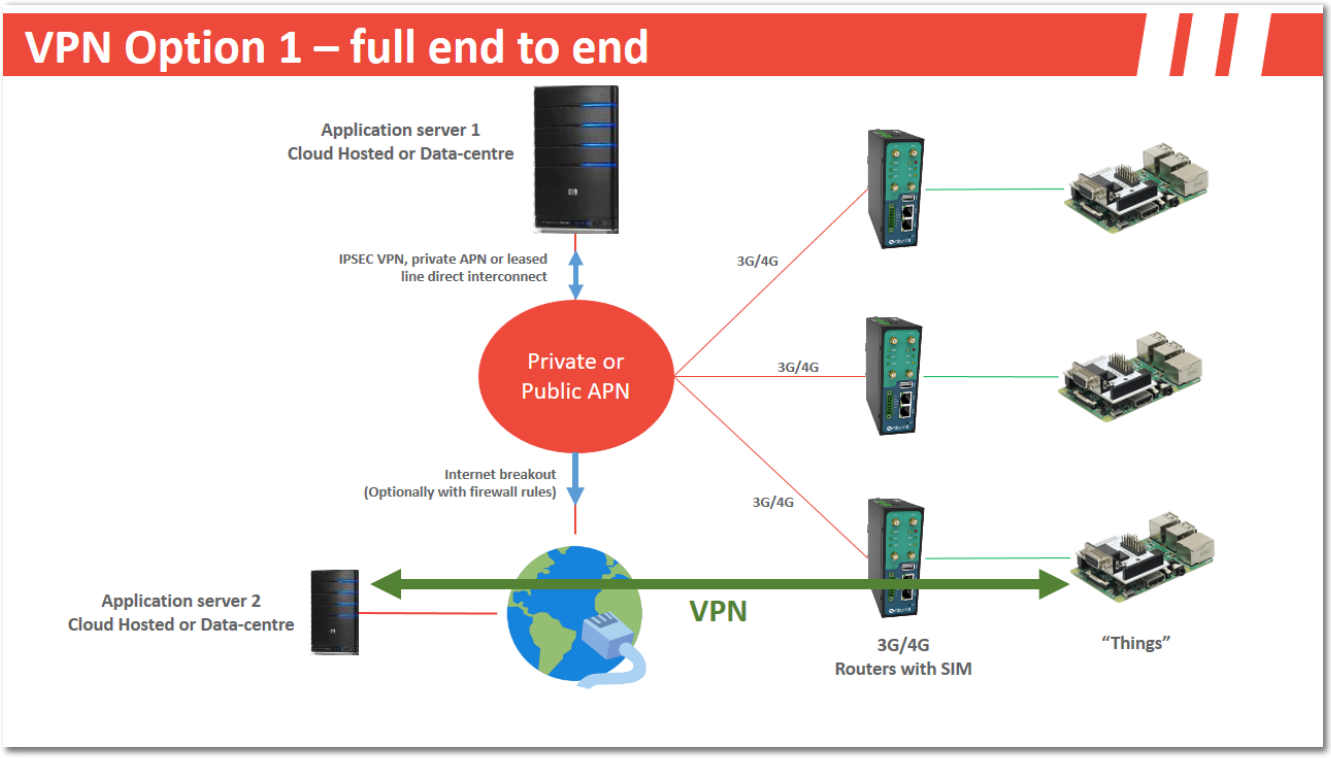

Figure 2.1 – end to end VPN from device to Cloud, through Operator's APN

In this example, the VPN traverses fully from the edge to the cloud, typically with the Thing at the edge running a VPN Client and the Application Server hosting a VPN Server for termination of the VPN connection.

In this example, there is no dependency on the SIM provider for this to work except that the chosen VPN type be allowed to traverse the operator's APN. This can be a key stumbling point that is worth checking with your SIM provider before trying to setup a connection.

Real-world deployments of this type of connection would generally use a VPN appliance just in front of the application server to provide a logical demarcation of the network building blocks.

Many "Things" do not have the capability of behaving as a VPN endpoint (such as an RS232 device) and in this instance, option (b) might be used.

Tip #6 – Some APNs can block specific ports or protocols in exactly the same way as a firewall would. Check with your SIM provider whether this is the case with their APN

b) Router to Cloud VPN

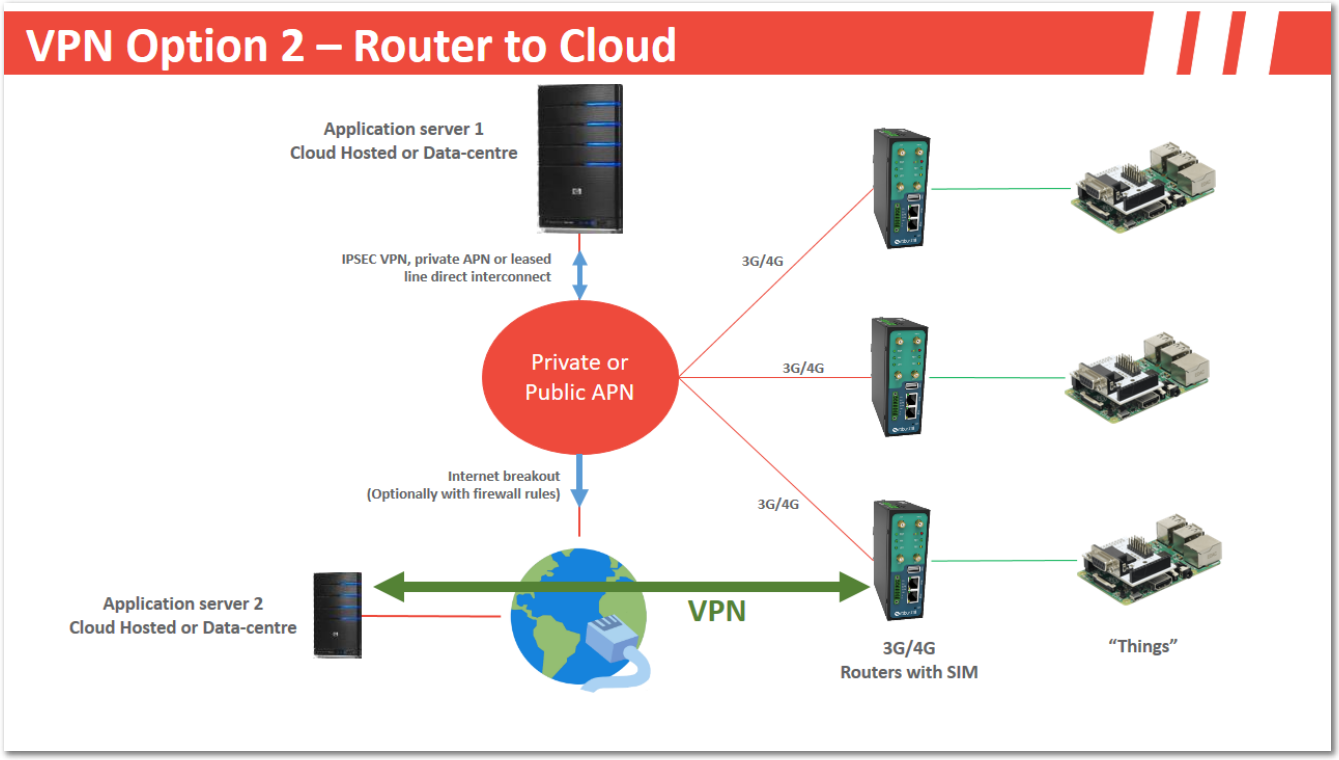

Figure 2.2 – Router to Cloud VPN – data between Thing and Router is unencrypted

In this example, the VPN traverses from the router to the cloud (Application Server or VPN appliance in the cloud) which in many ways is a more logical use of resources than (a) – allowing the Thing to be as cheap / dumb as possible and the Router to take care of the communication element.

On rare occasions, you will fall foul of the more pedantic of security auditors who insist that by use of the architecture above, the data going across the cable from the Thing to the Router is not covered by a VPN and so it poses a security risk. Common ways to deal with that objection are:

i – implement application layer security instead or as well as a VPN so the Thing to Router data is encrypted

ii – suggest that if someone has gained physical access to the router and the interconnecting cable then you have "bigger fish to fry" than worrying about whether they can see your bits and bytes!

This is a good reminder of Security being a cost/benefit equation and whilst option (ii) is a reasonable argument for some applications, it is unlikely to be acceptable in Medical or Military projects.

c) Use VPN solution provided by specialist M2M SIM card provider

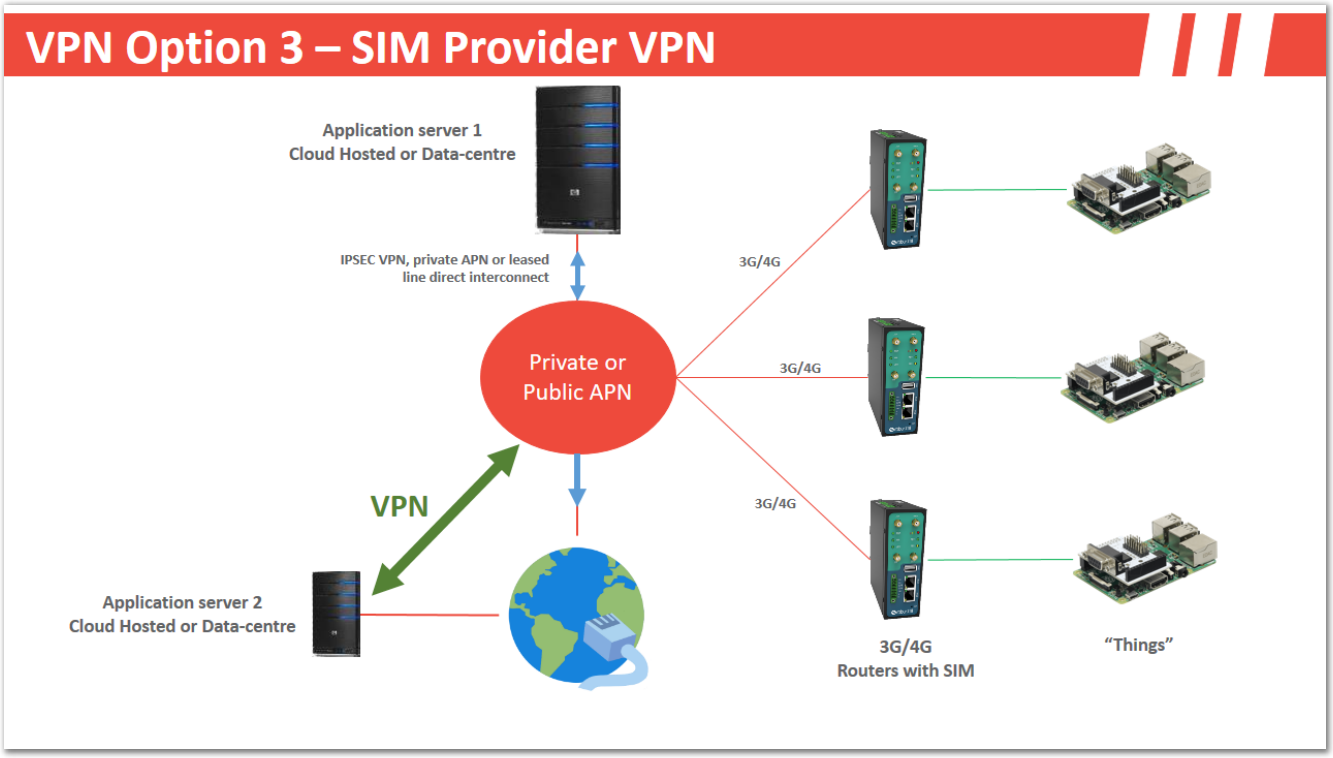

Figure 2.3 – SIM Provider's VPN Solution typically requires a single IPSEC from their APN to you

This type of service is commonly offered by MVNOs who want to enhance their service offering to customers and take on more of the solution in return for a small fee.

In most instances, an IPSEC VPN tunnel needs to be built between the SIM provider's APN and the Customer's VPN appliance / Server. Dual IPSECs can be setup for resilience at the cost of additional architectural complexity.

There are pros and cons to this solution as follows:

Pros

i) Zero changes need to be made to Router or Thing.

ii) Customer does not have to entertain the prospect of terminating many VPNs (one from each router) – just need one site to site VPN from the SIM Provider's infrastructure.

iii) Setup can be quite easy if SIM Provider provides good support.

Cons

i) VPN does not cover the air portion of the connection meaning that cracking of radio technologies could leave your data unprotected – a real objection but rarely upheld.

ii) If your SIM provider does a bad job then your entire estate of devices is at risk!

Section 5 – Robustel-specific Security Considerations

A. RCMS Cloud Platform

Robustel's primary strategy to secure its own router management service - RCMS, is to leverage the world-class IaaS and SaaS capabilities provided by Microsoft Azure.

An in-depth tutorial is available on how RCMS application software has a multi-layered defense against cyber-attacks courtesy of deep integration with the Microsoft Azure platform. A copy of the document is available on request from your Robustel sales representative.

B. Router Operating System (RobustOS) considerations

i) Software life cycle traceability

Robustel Incorporate security into all stages of the software development life cycle, including firmware design, secure storage and traceability of source code, and code review and analysis.

ii) Radius, Tacacs Plus, LDAP, LDAP X509 Authentication

Support for third-party server authentication, with flexible authentication mechanisms. The interaction between the client and the server is verified by a shared key & any user password transmitted is encrypted.

iii) Software life cycle traceability

Incorporate security into all stages of the software development life cycle, including firmware design, secure storage and traceability of source code, as well as code review and analysis.

iv) Encrypted diagnostic file

The exportable diagnostic file contains log + config information and is fully encrypted so it can be shared with Robustel Tech Support team for analysis without the possibility of compromise.

v) User roles management

Multi-role management, different roles have different level of management authority. "Guest" account can only see the device status – read-only. "Editor" can read/write but does not have user management permissions. “Administrator” has all administrative rights.

vi) E-mail TLS encryption

When event reminders are notified via email, data is transmitted under the TLS protocol, providing confidentiality and data integrity.

vii) Modbus data TLS encryption

In industrial applications, the collected data can be very sensitive. Modbus RTU data is transmitted to your server by MQTT wrapped in TLS for maximum security. A good example of application layer security. NB – requires “Modbus MQTT” app installed in RobustOS.

viii) Packet filtering firewall + DMZ

Filter data packets by IP, MAC address, protocol, and monitor each forwarded IP packet to keep the internal network secure.

IF you would like more information on IoT Security or details of Robustel’s products, please visit www.robustel.com or email info@robustel.com