Gallagher Command Centre

Mobile App – Network Deployment Options

Technical Information Paper

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Except where stated otherwise, the information is subject to copyright owned by Gallagher Group and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Contents

1 Background

The best network configuration for a Command Centre system will depend on many factors, such as the security concern for the site, the availability of skilled IT staff, and existing technology infrastructure. This document presents the various options and explains their benefits and risks to help guide decision making. It is meant to complement the **Command Centre Mobile App Security Technical Information Paper**, and as such does not discuss implementation details in great depth.

This document references version 7.70 and 8.60 of the Command Centre Server.
Command Centre 7.70 enables a new "Signed Token" Device Identification mode which allows traffic to be routed through a generic reverse proxy server.
Command Centre 8.60 enables the Gallagher Cloud API Gateway, which allows traffic to be routed through the Gallagher Cloud, enabling secure access over the internet.

If you are working with a newer version of Command Centre, please contact your Gallagher representative to confirm if this document is still relevant.

For guidance when deploying version 7.60 or older of Command Centre, please use the previous revision of this document provided with that Command Centre mode.

2 Identified Risks

1. **Denial-of-service (DOS) attack:** Attackers send an overwhelming amount of data to a network port. Having to process this data can degrade the performance of a server (potentially rendering it inaccessible). DOS attacks are the most common form of attack on the internet, as they require a lot of resource, but relatively little skill or targeted research.

2. **Low-level attack:** Attackers attempt to exploit vulnerabilities in the server operating system or hardware in order to crash or compromise the server by sending it deliberately malformed data. Low-level attacks are increasingly infrequent as modern software and operating systems improve, however when they do occur they can target a large class of targets (e.g. all Windows Server) in a broad sweep, so may have a wide impact.

3. **Application-level attack:** Attackers attempt to exploit vulnerabilities in the Command Centre Server software (or third-party software it may use) by sending it deliberately malformed data. Application-level attacks require knowledge of the target software, and in many cases may require special-purpose attack code crafted for the target system. They require the most skill and determination for an attacker to exploit.

3 Network Usage and Device Identification Mode

As mentioned in the Command Centre Mobile App Security Technical Information Paper, when configured to connect directly to the server, the Command Centre server uses two TCP ports to support Mobile Clients. The **Data** port (default 8901) and the **Enrolment** port (8902).

Command Centre will only activate the enrolment port when there are outstanding mobile devices to be enrolled. As soon as all devices are enrolled (or the enrolments expire 24 hours after issuance), the Command Centre server will shut down the enrolment port, eliminating this attack vector.

The system can be configured to either route traffic directly to the Command Centre server, or through an HTTPS reverse proxy to these ports, depending on the customer's IT capabilities and requirements.

If using a reverse proxy, you must configure the Command Centre server to use the **Signed Token** device identification mode. If you are not using a reverse proxy, you should configure Command Centre to use the **TLS Client Certificate** device identification mode, as it provides greater security (at the cost of not being compatible with reverse proxy solutions).

When using the Gallagher Cloud API Gateway, the above does not apply and all network connectivity and security is managed by Gallagher's cloud services.

Please refer to the API Gateway Technical Information paper for more detailed information:
https://gallaghersecurity.github.io/r/commandcentre-cloud-api-gateway

4 Vulnerability Overview – TLS Client Certificate Mode

TLS client certificate mode requires a direct network connection to the Command Centre Server, thus both ports are always exposed to DOS or low-level attacks.

While active, the enrolment port is exposed to application-level attacks as it must accept traffic from untrusted clients during enrolment. It only accepts a very small amount of specifically-structured data, and will reject anything else, so this risk is very small.

TLS client certificates prevent the data port from accepting any data from untrusted devices. This is validated by the Operating System, so untrusted devices will be blocked before being able to reach application code. Therefore the data port is protected from application-level attacks.

Note: This document assumes that trusted devices (mobile devices which have successfully enrolled with the server) will not attack the server. For this to occur, the attack would need to be performed by internal staff, or by a stolen device that has been left as trusted by the server. This kind of attack is also technically quite difficult to do and would require a lot of time and commitment in addition to a stolen device.

5 Vulnerability Overview – Signed Token Mode

When using Signed Token mode, a reverse proxy can be employed to form a barrier against DOS and low-level attacks, so both ports are always protected from these attacks.

As above, the enrolment port is theoretically vulnerable to application-level attacks while it is active, however this risk is very small.

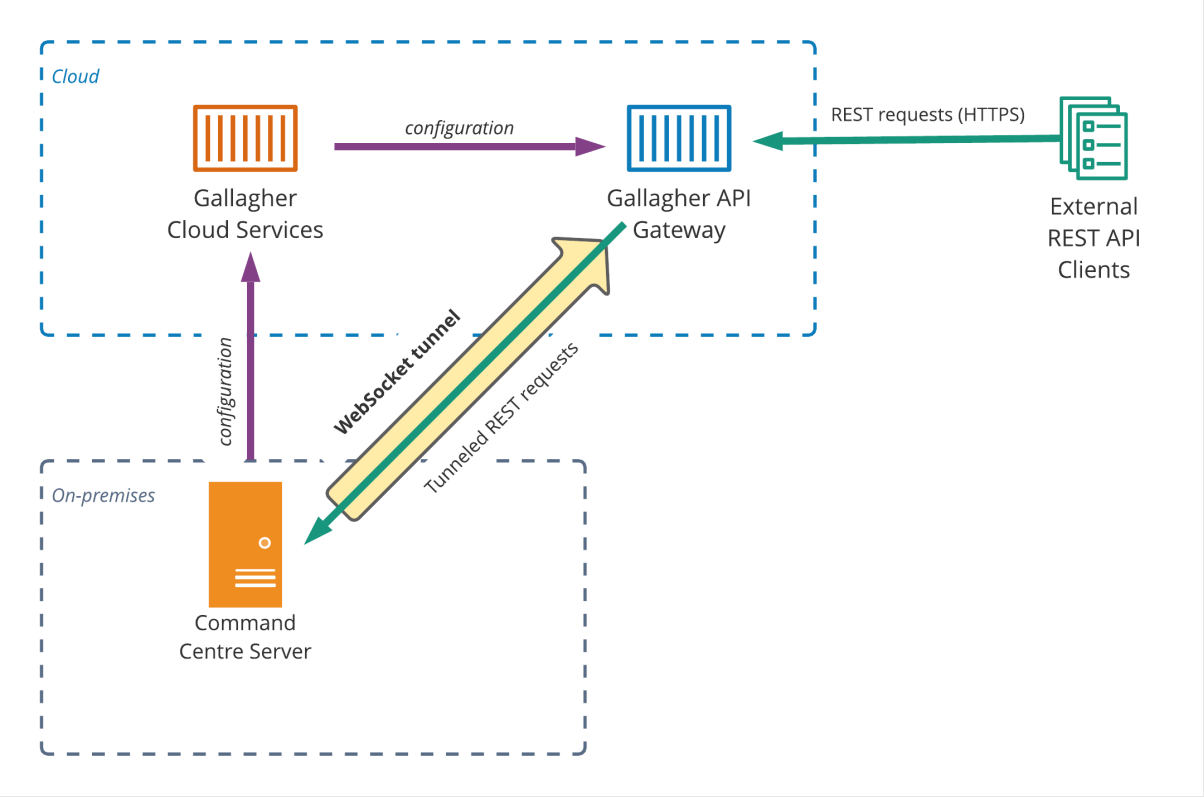
When in Signed Token mode, the Command Centre server requires valid credentials before it will accept any requests, however device and credential identification is performed by Application code in the Command Centre server, so the data port is exposed to application-level attacks.

Some reverse proxy software is capable of mitigating some kinds of application-level attacks.

If traffic is **not** routed through a reverse proxy, you should **not** use Signed Token mode, as you are exposing the server to application-level attacks on the data port without the benefit of the reverse proxy to mitigate DOS and low-level attacks.

6 Vulnerability Overview – Gallagher Cloud API Gateway

When using the Gateway, Command Centre Mobile applications will connect to Gallagher's cloud services. Messages are then relayed to the local Command Centre server via a websocket tunnel, which is outbound from the server to the cloud.



You may use the Gateway in a "Hybrid" configuration – where some mobile phones connect directly to the server, and others use the Gateway.

If you have a hybrid configuration, then all the vulnerabilities posed by either TLS Client Certificate, or Signed Token mode will apply to your server. If, however you *only* use the Gateway, then you can completely disable the local network ports used for the Mobile Client.

A vulnerability model for a "Gateway Only" deployment is as follows:

Denial of Service and Low-level attacks will be blocked or absorbed by Gallagher's cloud services. Whilst this may cause loss of service for your mobile applications, other side effects such as high CPU load, or network saturation of your local server, become impossible.

A critical benefit provided by the Gateway is that it removes the risk of older or unpatched software that is often exploited by low-level network attacks. For example, if you have a Command Centre server running on an older version of Windows or .NET, it may contain a vulnerability in some SSL or network layer code. Such vulnerabilities are common and require regular patching of all parts of the system (both Windows, and Command Centre) to mitigate. The Gateway, however, is a managed cloud service, and is continuously updated. If such a low-level vulnerability is discovered; Gallagher will patch it immediately in the cloud, and your server remains shielded.

Application-level attacks are still possible but become more difficult to achieve. The Gateway will authenticate all clients before forwarding any requests to your local server, so while some attacks are still possible, an attacker must first obtain valid authentication credentials. If you discover a compromised credential, you can revoke it and instantly prevent these attacks from reaching your server.

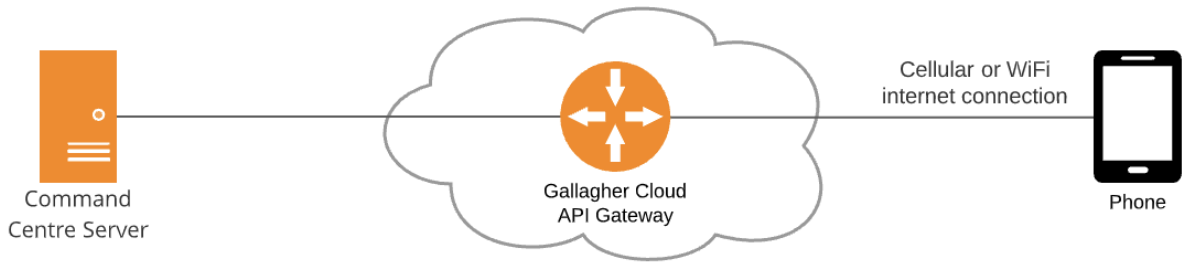
A hypothetical risk of using the Gateway is that if Gallagher's cloud services were to become compromised, a cloud-based attacker would be able to observe and manipulate data that passed through the Gateway.

For this reason, the Command Centre Mobile app uses end-to-end encryption when sending traffic through the Gateway. This makes it impossible for Gallagher (or any attacker who might have compromised Gallagher's cloud services) to observe or manipulate your data in this way. This also reduces the need for "inspection" solutions such as Web Application Firewalls, because end-to-end encryption ensures that the data received by your server is guaranteed to be the exact data sent from the mobile phone, without possibility of tampering by an intermediary.

For more detailed information on end-to-end encryption, please refer to the following Technical Information Paper: https://gallaghersecurity.github.io/r/mobileconnect-end-to-end-encryption

7 Deployment Options

7.1 Gallagher Cloud API Gateway Only



Best suited for most sites, with the following exceptions:

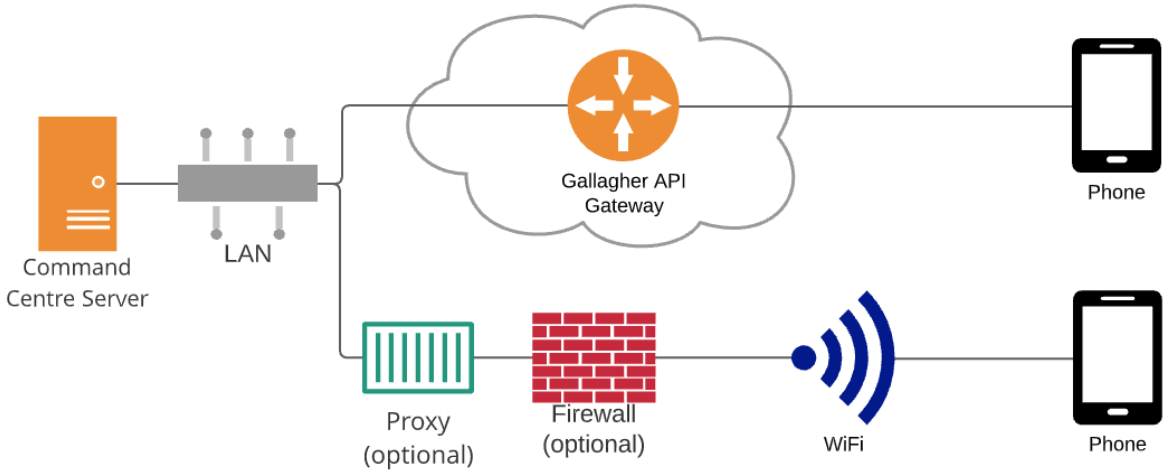
- Your site has some requirement to use additional custom authentication (such as that provided by a VPN appliance)
- Your site does not have an internet connection and therefore the Command Centre server cannot contact Gallagher's cloud services
- You have a specific requirement that certain mobile devices must only be used on a local network, to prevent them from being used offsite.
- Your site is running an older version of Command Centre before 8.60

Whilst the API Gateway requires an internet connection and is designed to enables secure off-site access, there is no problem in using the API Gateway on-site sometimes, or all the time.

The Command Centre mobile app uses a small amount of data, and whilst the Gateway does add some network latency, in most cases this will not meaningfully impact performance.

- ✔ Disabling local network connectivity prevents any local network attacks
- ✔ Allows local and off-site access in a highly secure manner
- Cloud connectivity required
- ✔ Do not need to configure local firewalls/networks at all (other than allowing the Command Centre server outbound access to the cloud)

7.2 Hybrid Cloud API Gateway / Local WiFi

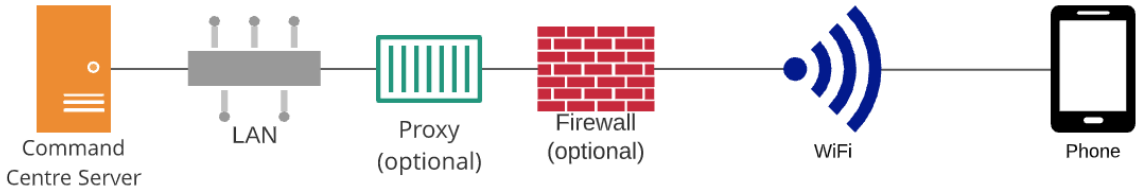


Best suited for sites who would like off-site Gateway access, but only for specific phones, whilst maintaining a second set of phones that are forced to use Local WiFi and be on-site.

For the phones that require local network access, TLS Client Certificates without any other third-party proxy is the recommended option.

- ✔ The Gateway provides secure off-site access via the cloud
- ✔ Phones which are not configured to use the gateway can be restricted to operation while on-site
- ▶ Local Enrolment port exposed to application-level attacks via internal Wi-Fi (only while enrolments active).
- ▶ Server exposed to DOS or low-level attack on both Local ports via internal Wi-Fi.
- ▶ May expose other services on the server (Command Centre or Configuration Client) to attack via the Wi-Fi network if there is no firewall configured on the server, or between the wireless and wired network.

7.3 Wi-Fi Only (either mode; TLS Client Certificates without proxy recommended)



Best suited for sites with an internal Wi-Fi network with good coverage that do not want off-site access, or sites whose Command Centre servers are not permitted to access the cloud.
Ideally the Wi-Fi network will be secure and only allow existing known devices to connect.

- ✔ Limiting access only to internal Wi-Fi prevents any external attack.

- Cannot use the mobile client off-site or out of Wi-Fi coverage.

▶ Enrolment port exposed to application-level attacks via internal Wi-Fi (only while enrolments active).

Direct Connection with TLS Client Certificate:

The majority of corporate Wi-Fi networks Gallagher have encountered provide security by restricting devices that can connect to them, so it is unlikely that the server will be subject to DOS or low-level attack, and we recommend using a direct connection with TLS Client Certificates

▶ Server exposed to DOS or low-level attack on both ports via internal Wi-Fi.

▶ May expose other services on the server (Command Centre or Configuration Client) to attack via the Wi-Fi network if there is no firewall configured on the server, or between the wireless and wired network.

Reverse Proxy with Signed Token:

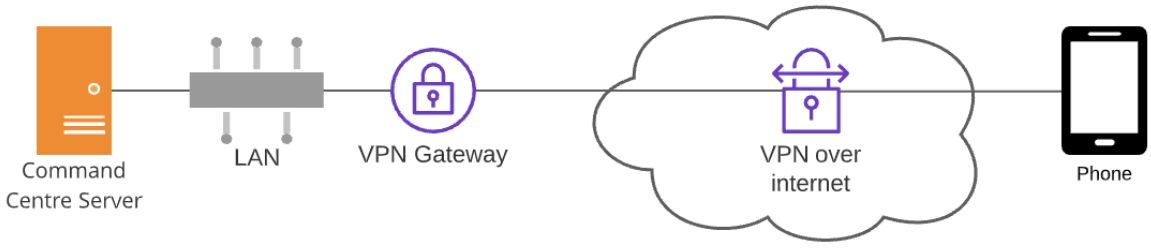
✔ Server protected from DOS or low-level attack on both ports via internal Wi-Fi.

▶ Data port exposed to application-level attacks via internal Wi-Fi.

✘ Requires additional work to configure reverse proxy.

7.4 VPN Over Internet (TLS Client Certificate mode)

VPN technology effectively allows remote devices to act as though they were connected to the local network over the internet.



Best suited for sites with existing VPN gateways that would prefer to use these for other reasons. For example, if the VPN gateway adds a second layer of authentication over the top of the mobile app.

If you are considering using VPN over Internet to allow connectivity from outside a local WiFi network, then the Gallagher API Gateway is likely to be a better solution.

It is possible to add both a firewall and a reverse proxy, however in most situations the VPN gateway can serve both those roles. In this mode, Gallagher recommend deploying in TLS Client Certificate mode without a reverse proxy.

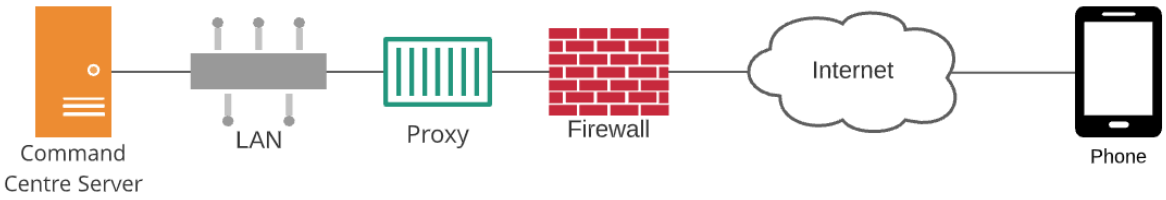
✔ Can use the mobile client anywhere there is cellular coverage.

- ✔ Limiting access only to the VPN prevents external attacks (unless the VPN itself is compromised).
- ✔ Server is only exposed to attacks from VPN-enabled devices, which will have already been approved and trusted.
- ▶ VPN may be difficult to configure or awkward to use (or expensive for sites which do not already have one).

7.5 Not Recommended: VPN Over Cellular (Signed Token Mode)

The VPN gateway will usually already provide network security. Enabling signed token mode to go through a secondary proxy will remove the benefits provided by TLS client certificates for no effective benefit.

7.6 Internet Direct Cellular with Reverse Proxy (Signed Token Mode)



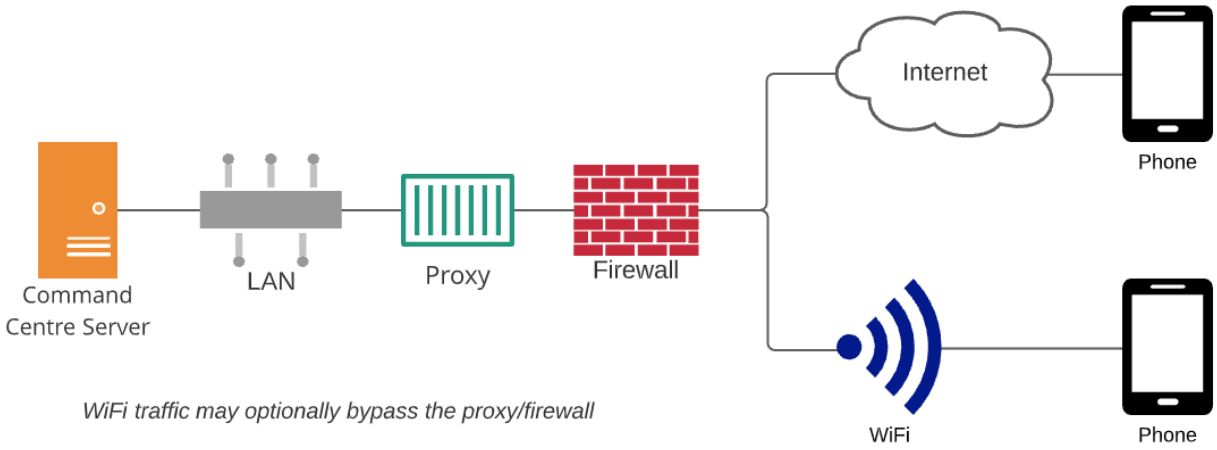
For sites using Command Centre 8.60 or newer, it is almost always better to use the Gallagher API Gateway in this scenario.
The only reason a site might choose to use this is if they had some specific proxy that was doing traffic inspection that was required for some policy reason.
For older installations this is best suited for sites that are required to use a specific proxy, or for sites that want to use the Mobile client offsite, without the expense or complexity of a VPN, and who accept the security risks.

- ✔ Can use the mobile client anywhere there is network coverage.
- ✔ Does not require a VPN solution to be configured.
- ✔ Reverse proxy provides defence against low-level and DOS attacks via the internet.
- ▶ Enrolment port exposed to application-level attacks via the Internet (only while enrolments active).
- ▶ Data port exposed to application-level attacks via the Internet (depending on type, the reverse proxy may be able to mitigate or block some of these).

7.7 Not Recommended: Internet Direct Cellular Without Reverse Proxy

This would expose the server to DOS + low-level attacks from the internet, which are the most common types of attacks present on the internet.

7.8 Internet Direct Cellular + Wi-Fi With Reverse Proxy (Signed Token Mode)

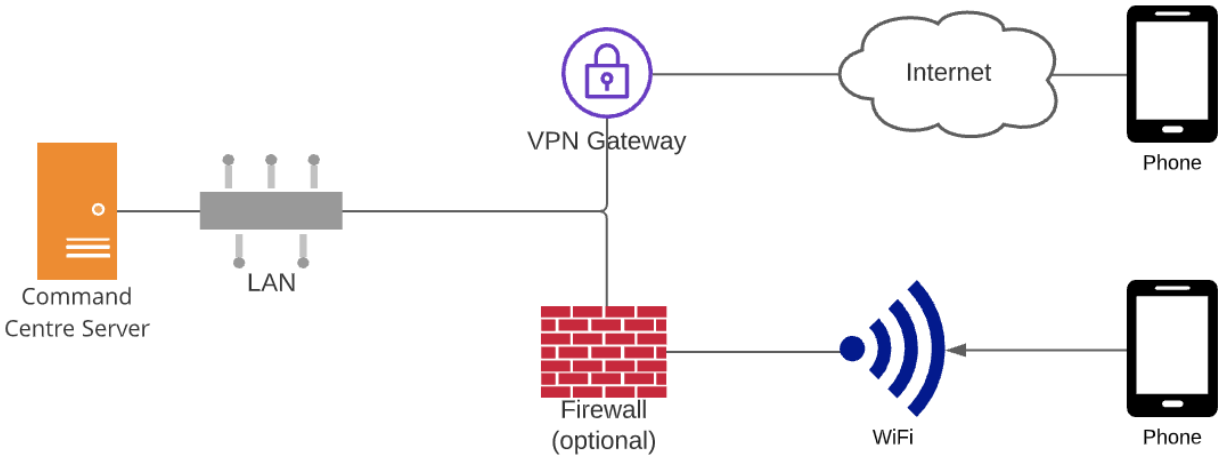


For sites using Command Centre 8.60 or newer, it is almost always better to use the Gallagher API Gateway in this scenario.

For older installations this is best suited to sites which cannot or do not wish to use a VPN, but still require off-site access using the Mobile Client, and have internal Wi-Fi.

- The mobile client generally does not use a lot of data. If cost savings are the only motivator for adopting this model over cellular only, it is unlikely to be worth it.
- ✔ Can use the mobile client anywhere there is cellular coverage.
- ✔ Does not require a VPN solution to be configured.
- ▶ Enrolment port exposed to application-level attacks via the Internet (only while active).
- ✔ All Internet attacks against the enrolment port can be prevented by blocking the enrolment port externally. The enrolment port can be left enabled on Wi-Fi.
- ✔ Reverse proxy provides defence against low-level and DOS attacks via the internet or Wi-Fi.
- ▶ Data port exposed to application-level attacks via the Internet or Wi-Fi.

7.9 VPN Over Cellular + Wi-Fi (TLS Client Certificate Mode)



This may be desirable if the site wishes to sometimes allow internet access via a VPN but would like to use internal Wi-Fi when on site.

- The mobile client generally does not use a lot of data. If cost savings are the only motivator for adopting this model over VPN only, it may not be worth it.

✔ External attacks are prevented by Wi-Fi and VPN models.

✔ If the mobile devices are not permanently connected to the VPN, and connecting to the VPN is annoying or troublesome, this lets the devices be used without VPN on the secure internal network.

- The network needs to be configured to allow phones to switch between the VPN and Wi-Fi while preserving their server settings (the server IP address or DNS name must appear the same from both networks).

7.10 Not Recommended: Internet Direct Cellular + VPN Over Cellular

This does not offer any advantage over internet direct cellular and is harder to configure.

7.11 Not Recommended: Internet Direct Cellular + VPN Over Cellular + Wi-Fi

This does not offer any advantage over internet direct cellular + Wi-Fi and is harder to configure.