wifi wall

White Paper WifiWall 2.4GHz

14.2.2019

How It works?

Wifi Attacks varies from an attacker using a station in the Wifi network, cracking the password, hijack station connections, constitute a man in the middle, etc. Wifi attack may also start "outside" the network such as Evil Twin or Rogue Access Point, etc.

WifiWall is designed to detect and prevent both, inside or outside Wifi attacks.

The trigger to develop WifiWall was the sensational news of KRACK attack, in October 2017. Until then, everyone believed that WPA2 encryption is doing an excellent job after WEP, and WPA failures. This changed with the KRACK that allows researchers an attacker to crack WPA2 passwords in less than two minutes. In 2018, it was improved to about 10 seconds....

While KRACK and other attacks pushed IEEE organization to quickly (mh... is this good?) design and release WPA3 definitions, it will take years to find WPA3 networks and devices everywhere.

Wigle.net mapped 521 Million Wifi routers and Access Point worldwide. Wigle.net reports that the WEP protocol released in 1997, is implemented on 6.31% of all Wifi Networks. If we focus only on public networks, this number rises to near 10% (2019 figures). This is 22 years after WEP released. It takes a while to upgrade infrastructure, even when it comes to networking.

When we designed WifiWall,
we came with the following major requirements:

1. Nonintrusive – A proxy solution (intrusive), requires to connect your phone, laptop or tablet (we call it Station in this article), to a proxy device that is connected to the router or AP. The proxy creates new challenges: it slows down the connection, it may also manipulate the content (filter function). Both actions quickly drive the user to remove the proxy and connect with no security at all. End users have no patience to slow down the connection. Therefore, we looked for a non-intrusive solution, one that no one can even blame for slowing down, performance degradation or content manipulation.
2. No Software install – A solution that doesn't require software on the station, means that it supports ALL types of stations: Android or Apple phones, Tablets, Windows PC, MAC OSX, printers, IoT devices, and even Wifi Camera! From day one, any Wifi 2.4GHz 802.11 devices are supported.
3. Switch on and Go – A solution that doesn't need complicated setup, customization or even registration to function. Just turn the switch on, and be protected.

While we see the value (3) a significant one, some users, ask us: "why not implementing the WifiWall as a phone App?" check below the answer for this question.
So, how do we do it?

WifiWall is a miniature computer, running two cores ARM, Wifi 2.4GHz and BT/BLE units. WifiWall constantly monitors all Wifi networks in the vicinity, which means that it intercepts all packets from all Routers, Access Point and Stations in the network.

The "relations" between the protected Station (Phone, Laptop, etc.) and the WifiWall are simply the MAC Address of the station. WifiWall 2.4GHz protects up to two stations simultaneously.

All WifiWall requires to "know" is the Mac addresses of these Stations. The way to "teach" WifiWall is also straightforward:

When a brand new WifiWall 2.4GHz starts (out of its box) it publishes "WifiWall_setup" network name. All you need to do is connect your Station to this Wifi network. That's it, WifiWall will save the Station's Mac address and will restart in "protecting" mode, meaning, monitoring the Wifi networks to detect attacks.

How WifiWall detect attacks?

Now that WifiWall "knows" your Station Mac address, it focuses on Wifi traffic to and from your Station. When your Station connects to a public or private 2.4GHz Wifi, WifiWall detects it and displays the name of the Wifi network on its display.

Now, let's check inside and outside attacks, and see how WifiWall performs in each:

Inside Attack:

In this attack type, the Attacker uses a station to sniff the network traffic, to crack the Wifi password or to set a man in the middle attack. By cracking the password and sniffing the traffic, the attacker can view all your content or manipulate it, examples:

Eavesdropping:

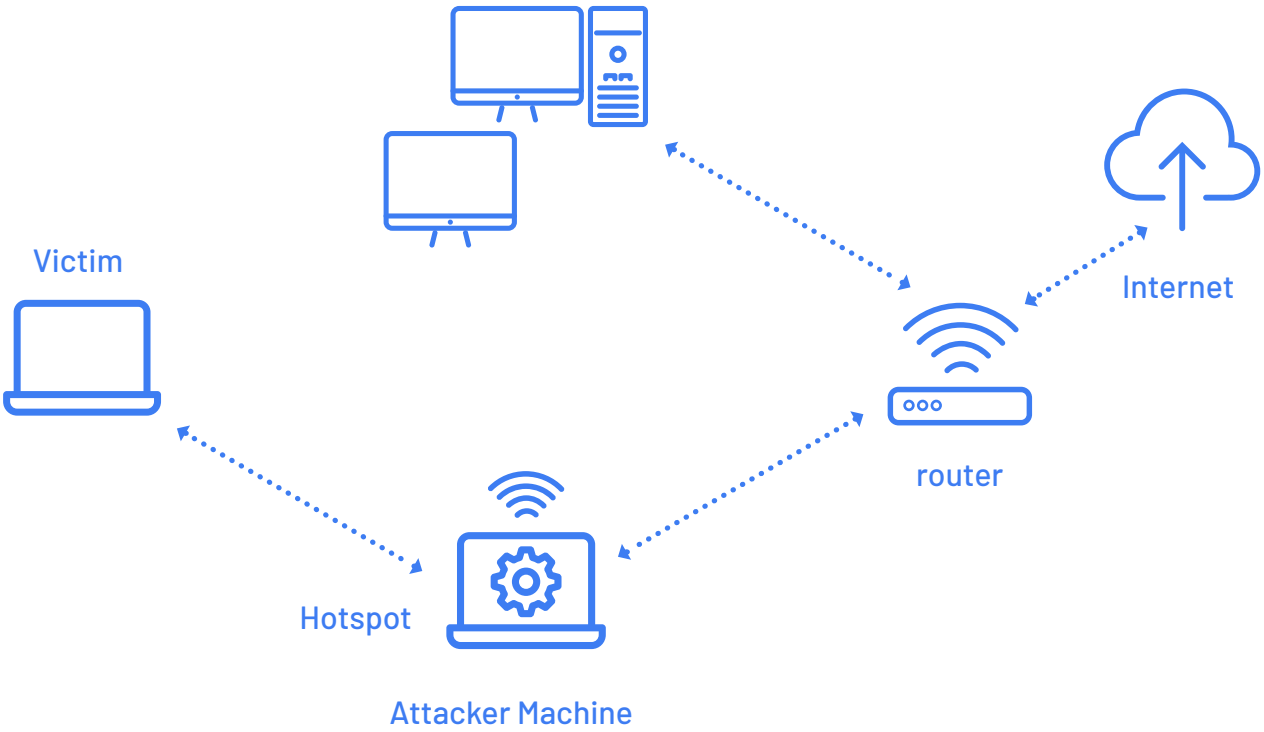
This is where someone tries to listen to the data transferred between clients and the access point. Its very easy with open networks, therefore, it is essential to encrypt your networks.

Password Cracking:

This is where the attacker attempts to crack the encryption on the network.
Using a smartphone or Laptop and professional Wifi Adaptor, the attacker can "sniff" all network traffic. The Attacker can use different tools such as WifiPhisher, Aircrack-ng, (its Android interface: "Hijacker v1.3 – A Complete Wi-Fi Hacking Tool Kit for Android"), Reave WPS cracker, and many other tools. The professional Attackers, build their tools or trade it in the Dark Web.

Men in The Middle Attack

The topology looks like:



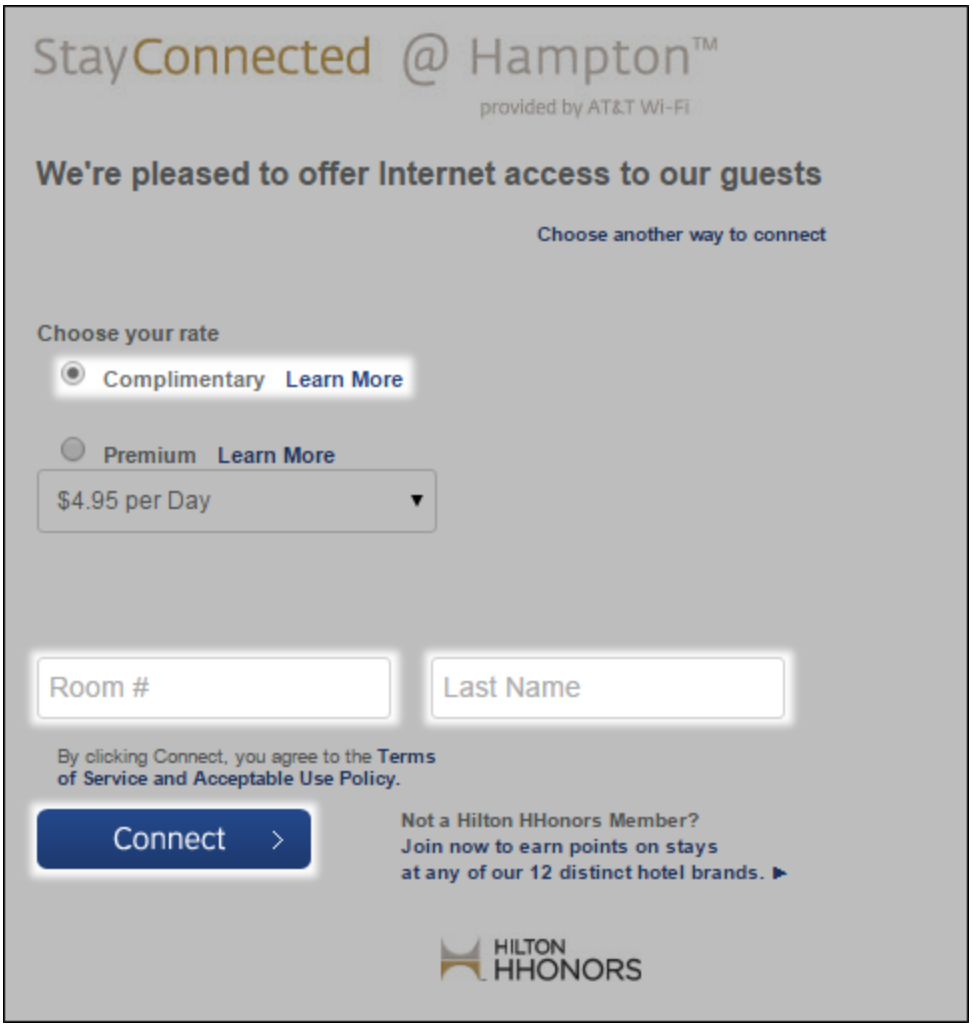
In this type of attacks, the Attacker sends De Authentication or De Association Frame to the victim. Why would this even happen?

Wifi networks are based on Radio Frequency (RF). These channels may suffer from low reception or high noise level, and therefore, from time to time, the Router or AP request the Station to switch a channel. This happens without any notification to the user, and very fast.

Since Wifi allows any station to send frames to other stations, the Attacker station can order the

victim's station to switch the channel. The Router is not aware of that and therefore will stay with the same channel, but the Attacker station will "wait" for the victim's station on the new channel, pretending to be the router. Now a new connection is established between the Victim's station and the Attacker station. Now the Attacker has many options:

If the original router sends a "splash screen" such as:

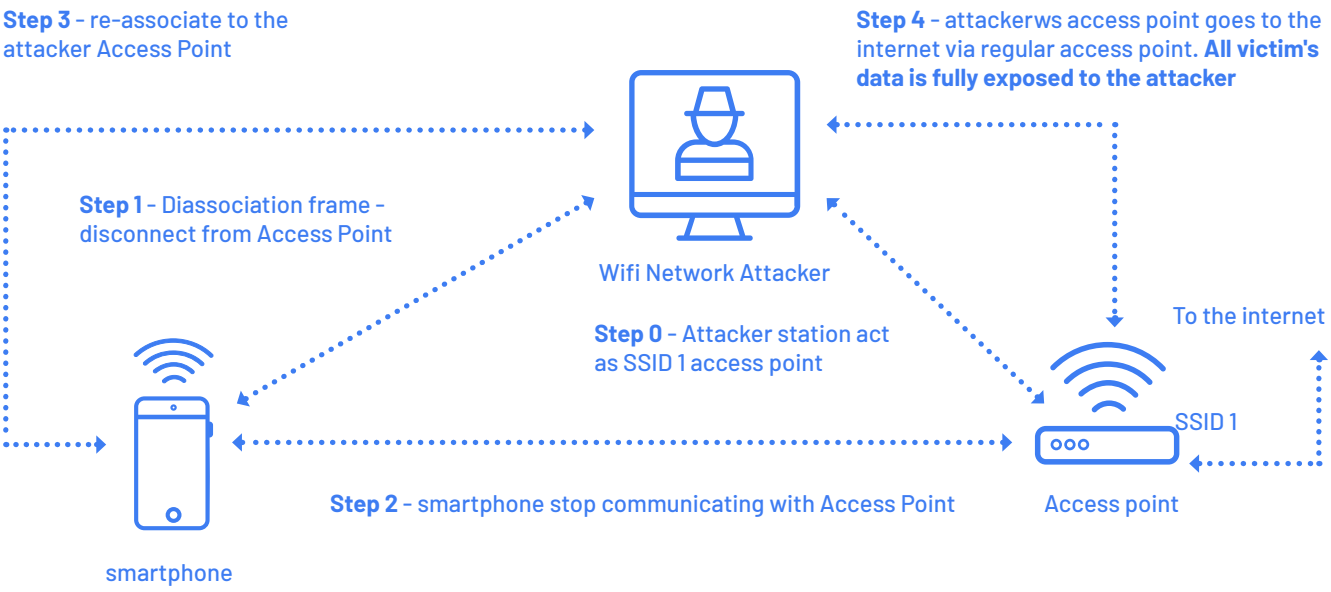


It can send a similar screen (actually HTML page) with invisible Malware as payload. This Malware will act a long time after the victim left the location.

Hijacking

Alternatively, Attacker may become a "proxy" for the victim's station, so it intercepts all victim's traffic, decrypted it with the cracked password, copy or modify it.

Hijack Wifi Communication Example



Management Interface Exploits

The Attacker uses the Router or AP Web Interface to control and manage. Default login credentials are widely available on the internet, so it's crucial to ensure that all devices are securely locked down to prevent unauthorized access. WifiWall 2.4GHz doesn't protect this kind of attacks.

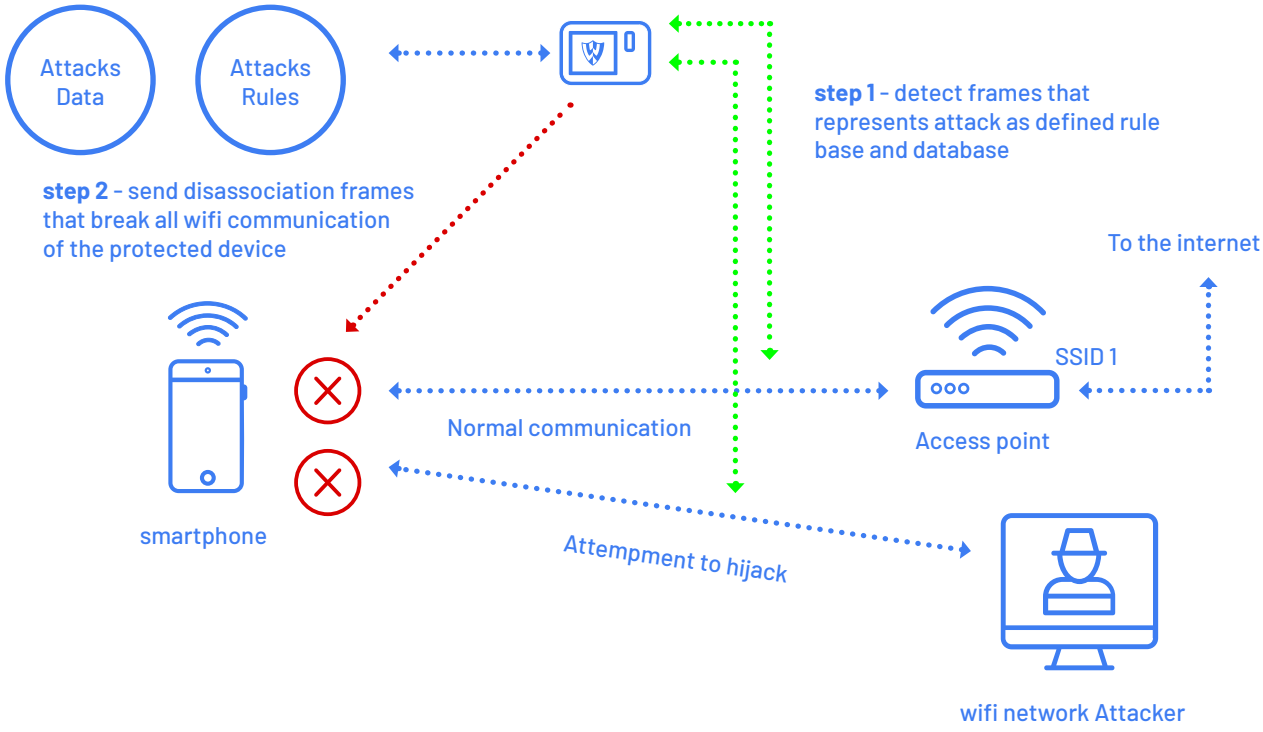
How WifiWall Protect against Inside Attacks

As mentioned, WifiWall monitors all Wifi traffic, focusing mostly on the Management and Control frames. It uses its built-in Protocol Distortion and Diversion Detector ("P3D") to detect any manipulation to the 802.11 protocols, diversions, or actions not expected by the Router or other Stations in the Wifi network.

In such a case, WifiWall 2.4GHz uses its built-in Attack rules and Attacks Data to identify the attack when it starts.

When the attack is identified and detected, WifiWall 2.4GHz alerts the user (using the device OLED screen) and send 802.11 frames to the victim's station requesting to end the current session.

This is done, without having a software agent on the station but by sending 802.11 control frames from WifiWall 2.4GHz directly to the victim's station.



Outside Attack:

These are the most frequent Wifi Attacks, known as Rogue Access Points, Evil Twin, Fake Access Point, etc. The Attacker can easily set up a Rogue AP often using the same name of the Wifi network (SSID). Alternatively, Attacker can use a luring name such as 'Free Airport WiFi' etc.

When the victim's station connect to such AP, the AP may divert the request to a splash screen (see the example above for inside Attack), using a captive HTML page and a built-in DNS server that redirect any call to this captive page.

The attacker may allow the victim's station to yet connect to the internet while not be aware that something is wrong. Of course, sensitive information entered online, such as email addresses and passwords, credit card numbers, or banking credentials can be stolen.

To create this Attack, the Attacker can use a laptop or Open source Wifi Router (a long list may be found at OpenWrt: https://openwrt.org/). This Evil Twin can have a very strong signal which may get more connection than the original Router and become a man in the middle for all traffic. This is one of the most common wireless network attacks, and it is surprisingly effective. About 20% of Wifi users will be connecting to a Rogue Access point while they travel.

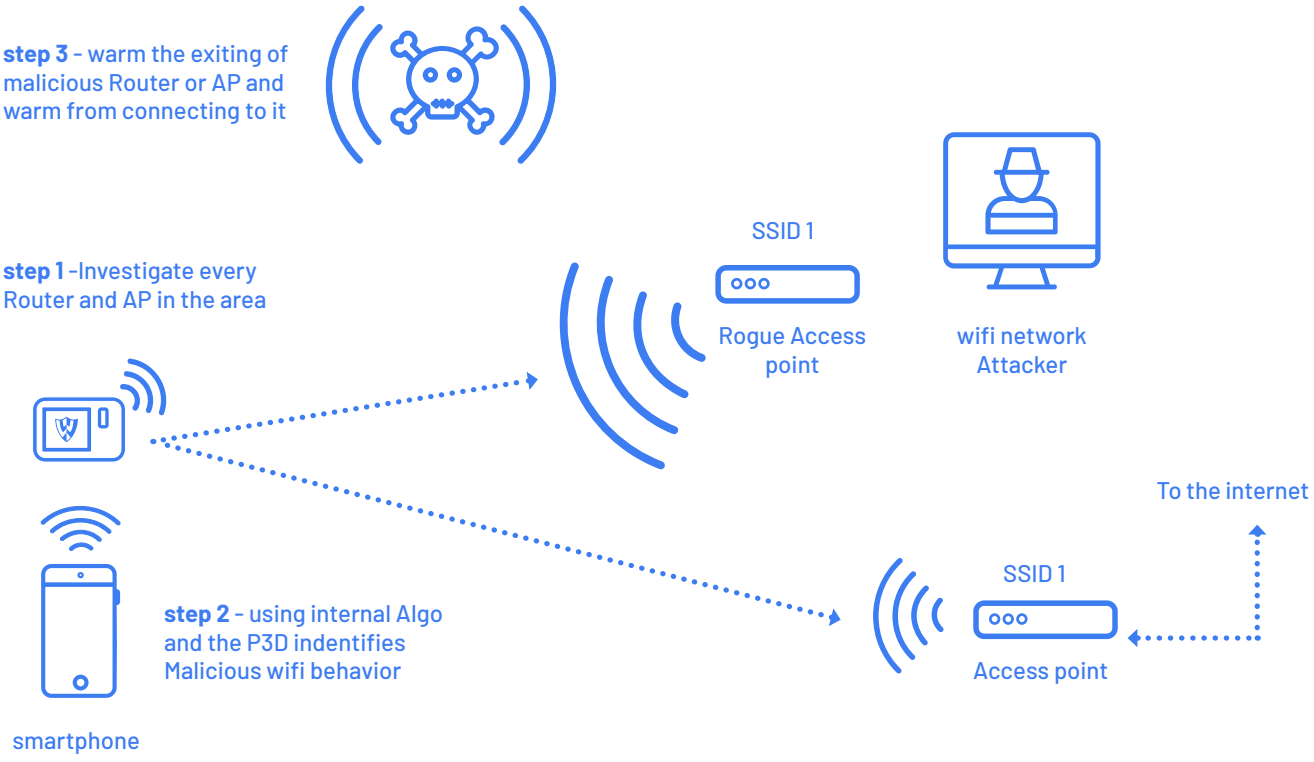
How WifiWall Protect against Outside Attacks

WifiWall 2.4GHz constantly monitors all Routers and AP in the vicinity. It regularly updates its internal AP DB with the details of every Router and AP in the area. It than monitor the traffic to and from these Routers and APs, investigating their relations (are they part of Mesh network?) and their internal setup.

The result of the investigation is a list of Routers or APs that are Evil Twin, Rogue AP, a man in the middle AP, etc.

When these malicious Routers and AP are detected in the area, WifiWall 2.4GHz warn the user about their presence.

WifiWall also detects an attempt of the user station to connect to such a malicious Router or AP. In that case, WifiWall notifies the user that his station attempt to connect to a malicious entity to avoid any damages from happening.



Why not implementing the WifiWall as a phone App?

WifiWall opens the Wifi network interface in monitoring mode. In this mode, the interface card intercepts every 802.11 frames and pass it to the central processor. There is no TCP/IP work at that level.

If we try to implement such a solution as a Phone App, the network performance of the phone will dramatically reduce to almost no internet connection.

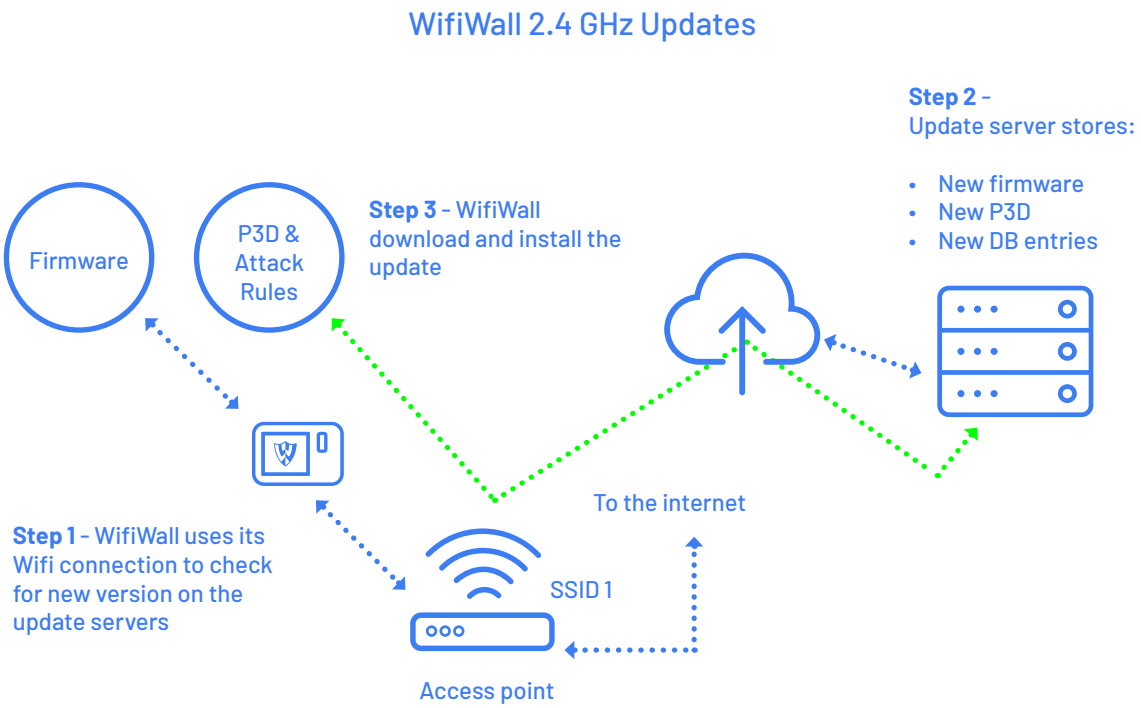
Therefore, a solution which is nonintrusive, that doesn't affect CPU or networking performance and doesn't require any agent on the phone, can be implemented on a separate Wifi entity.

We made it small, portable and durable.
We call it WifiWall 2.4GHz.

Updating WifiWall 2.4GHz

WifiWall 2.4GHz requires periodic updates to its software. This is done by the device using its remote update procedure. To check for update, WifiWall 2.4GHz requires a direct connection to a Wifi network.

To setup its Wifi connection, you need to download our Android or IOs App "WifiWall Connect", that can be found in the App stores. Check WifiWall 2.4GHz user manual for instructions on how to set WifiWall Wifi.



WifiWall 2.4GHz Anonymous Data Uploading

If and when WifiWall 2.4GHz connects to the internet apart from getting updates it also sends and receives the following information to/from its cloud servers:

1. Outside Attack details: i.e., Detection of Rogue AP – WifiWall sends the MAC address and SSID names of the detected malicious Router/AP to the cloud. If the cloud recognizes this Router/AP and stores additional relevant information, this information will be sent back to WifiWall 2.4GHz.
2. Inside Attack details: WifiWall sends attack report for every incident. The report includes the Mac address and SSID of the connected Router/AP, the victim's Mac address, WifiWall software version, and the attack descriptor.
3. Software update record. When the WifiWall completes software update, it notifies WifiWall update servers about it.

We plan to use this information in future Phone Application that will allow the user of WifiWall 2.4GHz to view the history of attack attempts on his devices, manage and display WifiWall parameters. We also plan to keep a record of Worldwide attacks database, that doesn't store any information on the victim's station (not even Mac address), just for sharing statistics with other WifiWall users and customers.